

INTRODUCTION TO DIGITAL FORENSICS

ဆရာများအား လေးစားဂုဏ်ပြုလျက်

Aung Zaw Myo

(ThirdEye)

www.forensicsmyanmar.com

Forensics myanamr

CERT ကနေအဓိပ္ပာယ်ဖွင့်ဆိုထားတာကတော့ ...Network or information System တစ်ခုကို ကိုင်တွယ်နေရသူတစ်ယောက်ဟာ Forensics အခြေခံကို နားလည်ရမယ်လို့ ဆိုပါတယ်။ ပိုမိုပြည်စုံအောင်ဖွင့်ဆိုမယ်ဆိုရင်သိပ္ပံနည်းပညာဆိုင်ရာအချက်အလက်တွေကို အသုံးပြုပြီး... အချက်အလက်တွေကိုစစ်ဆေးခြင်းသက်သေတွေကိုစုစည်းခြင်းတို့ဖြစ်ပါတယ်။ သက်သေတွေကို စုစည်းခြင်းဆိုတာကတော့ DNA Fingerprint တို့ကို စစ်ဆေးစုစည်းခြင်း ကဲ့သို့ဖြစ်ပါတယ်။ ဒီနေရာမှာကတော့ data တွေကို စစ်ဆေးပြီး သက်သေခံရှာ ဖွေခြင်းဖြစ်ပါတယ်။ Forensics မှာ အဓိက လုပ်ငန်းကတော့ ငုပ်လျှိုးနေတဲ့ အချက်အလက် တွေကို ရှာဖွေဖော်ထုတ်ခြင်း ဖြစ်ပါတယ်...ဖော်ထုတ်တယ်ဆိုတာမှာ RECOVERY လုပ်ခြင်း အပိုင်းအပါအဝင် နည်းအမျိုးမျိုး ရှိပါတယ်။

ဥပမာ... ကွန်ပျူတာပေါ်မှာကျန်ခဲ့တဲ့ လက်ဗွေ... DNA ယူခြင်းဟာလည်း Forensics အပိုင်းမှာ ပါဝင်ပါတယ်။

Digital Forensics မှာအဓိကအချက် ၂ရှိပါတယ်။

ပထမအချက်

ဖမ်းဆည်ရမဲ့သူဟာ.... Electronic Device ကိုသုံးပြီး ဘာတွေကျူးလွန်ထားလဲ .ဖမ်းဆည်းနေချိန်မှာ Electronic Device ကိုအသုံးပြုနေပြီး ဘာတွေ လုပ်ဆောင်နေသလဲ ဥပမာ online လောင်းကစားလုပ်နေတာလား စသည်ဖြစ်ပေါ့ ပြီးရင် Website ကိုအသုံးပြုပြီးလုပ်ဆောင်နေတာလား Software ကိုအသုံးပြုပြီးလုပ်ဆောင် နေတာ လားဆိုတာ ကြည့်ရပါမယ်။

.Electronic Deviceဆိုသည်မှာPC LaptopTablet mobile phone GPS CD DVD SD Card USB Router , Switch Server IOT device စသည်ဖြင့် ပါဝင်ပါတယ်.... (ဘာလို့ Internet of things (IOT) ကို ထည့်ရသလဲဆိုရင် IoT device တွေပေါ်ကနေ crime ကျူးလွန်နိုင်လို့ဖြစ်ပါတယ် ... အချို့သော နိုင်ငံတွေရဲ့ Cyber Law မှာ IOT Device အတွက်ပါ ထည့်သွင်းရေးဆွဲထားတာကို တွေ့ကရိရပါသည်။)

ဒုတိယအချက်

ပထမအချက် လုပ်ဆောင်ချက်တွေကို စစ်ဆေးပြီး တရားရုံးသို့ တင်နိုင်မဲ့ သက်သေခံ ယူရမှာဖြစ်ပါတယ်...အရေးကြီးတဲ့အချက် ၂ ချက်ကျန်ပါသေးတယ်။

ပထမ

စစ်ဆေးပြီး သက်သေခံရှာဖွေပြီး တာနဲ့မပီးသေးပါဘူး သက်သေခံ Device ကို မပျက်စီးအောင် သိမ်းဆည်းရမှာဖြစ်ပါတယ်...စစ်ဆေးတဲ့နေရာမှာလဲ သိမ်းဆည်းထားတဲ့ မူရင်း Device ကိုမပျက်စီးစေပဲ ဘယ်လိုထိမ်းသိမ်းမှာလဲ ဘယ်လိုမှတ်သားထားမှာလဲ Case အလိုက် ရက်စွဲ အလိုက်မှတ်သားထားမှာလား?

ဘယ်သူက ဘယ်နေ့၊ ဘယ်အချိန်မှာ ဘယ်လိုနည်းလမ်းအသုံးပြုပြီး စစ်ဆေးမှာလဲဆိုတာကိုလဲ ...အသေးစိတ် မှတ်တမ်းထားရှိရမှာဖြစ်ပါတယ်။

(သိမ်းဆည်းစဉ်မှာ အခြေအနေအရ စစ်ဆေးတာ သက်သေယူတာက မပြီးသေးဘူးဆိုရင် ... Device ကို Power ပိတ်ယူမှာလား ...ဖွင့်ယူမှာလားရှိပါသေးတယ် .. Computer Forensic အပိုင်းကျမှ အသေးစိတ်ဖြစ်အောင် ရေးသားပါမယ်)

ဒုတိယ....

ရရှိလာတဲ့သက်သေတွေကို ရှင်းရှင်းလင်းလင်း ခိုင်ခိုင်လုံလုံဖြစ်အောင်ရေး မယ် ... ပြီးရင် သက်သေခံ Device နဲ့တစ်ကွ တရားရုံကို တင်မယ် ..

နောက် post တွေမှာ Example ပုံစံတွေ အသေးစိတ်လိုက်နာရမဲ့အပိုင်းတွေ စစ်ဆေးရမဲ့ နည်းလမ်းတွေ(အကျဉ်းချုပ်ပေါ့)ကိုရေးသားပေးပါမယ်..

Hypothesis လို့ခေါ်တဲ့ ထင်မြင် ယူဆချက်အကြောင်းကတော့

Case တစ်ခုအတွက်ဖမ်းဆီးပြီး သက်သေခံ Device (Laptop ပဲဆိုကြပါစို့.) ကိုသိမ်းထားလိုက်ပြီး ဥပမာ ... ကလေးသူငယ်ပုံတွေကိုတင်ပြီး အွန်လိုင်းကနေ လိင်အကြမ်းဖက်လုပ်ဆောင်တဲ့အမှုပေါ့

(သိမ်းဆည်းနည်း စစ်ဆေးနည်း အကျဉ်းကို PART 1 မှာရေးပြီးပါပြီ)လုပ်ဆောင်တဲ့သူက ဒီလူပဲ ဆိုတာလဲသေချာသလောက်ရှိနေပြီး.... laptop ကိုအသုံးပြုပြီး ပြစ်မှုကျူးလွန်တယ် လို့လဲ ယူဆတယ်....ခက်တာကသိမ်းဆည်းမိတဲ့LaptopကWindow ပြန်တင်ထားတာမကြာသေးဘူး ကဲယူ ဆချက်တော့ရှိပြီးသက်သေခံအချက်အလက်ကမရသေးဘူး....ကဲ.. ဘာလုပ်မလဲ laptop အသုံးပြုထားတဲ့ Time ... Window ပြန်တင်ထားတဲ့အချိန်ကို ကြည့်မယ် ပြီးရင် Storage Device ဖြစ်တဲ့ Hard Disk ဒါမှမဟုတ် SSD ပေါ့ အဲဒါတွေရဲ့ Power On Time စစ်မယ် ...

HD or SSD ရဲ့ Health ကိုစစ်မယ် စစ်ဆေးနေတုန်း... HD ကြွသွားရင် လုံးဝ အဆင်မပြေနိုင်ဘူးလေ....

အရေးအကြီးဆုံးအချက်ကတော့ ... မူရင်း HD or SSD ကနေ Clone ယူပြီး စစ်ဆေးတာ အကောင်းဆုံး နည်းလမ်းဖြစ်ပါတယ် ...ဒါမှ သက်သေခံလဲ မပျက်စီးပဲ တရားရုံးမှာပြနိုင်မယ်

အခြေအနေအရ clone ပဲယူယူ .. မူရင်းကိုပဲစစ်စစ် Recovery တွေ Undelete နည်းလမ်းတွေနဲ့ အဆင်မပြေဘူးကဲ ... ဘာလုပ်မလဲ ထင်မြင်ယူဆတာနဲ့လွဲနေပြီး ဒါဆိုရင် ကိုယ်က ဘယ်လိုနည်းလမ်း တွေအသုံးပြုပြီးပြီးလဲနောက်ထပ် သိပ္ပံနည်းကျ ဘယ်လိုနည်း လမ်း တွေကို အသုံးပြုပြီး သက်သေခံရအောင်ယူမလဲ မိမိကျွမ်းကျင်မှု အလိုက်အသုံးပြုမှာဖြစ်ပါတယ်

Forensicsနည်းပညာထွန်းကားလာပုံ

1822-1911 ကာလအတွင်းမှာတော့ လက်ငွေ့နည်း စနစ် စတင်ပြီးတိုးတက်လာပါတယ် ...

1847-1915 criminal investigation တစ်ခုဖြစ်တဲ့ မူခင်းဖြစ်ရပ်တစ်ခုကို စစ်ဆေးကာ သက်သေရရှိမှုအပေါ်မူတည်ပြီး တရားခံကို ရုပ်လုံးဖော်ခြင်း ပညာရပ်ဟာ တိုးတက်လာပါတယ် ...

1858-1946 လက်ရေး လက်မှတ် စာရွက်စာတမ်း အတု ဖြစ်မဖြစ် စစ်ဆေးတဲ့ နည်းပညာဟာ တိုးတက်လာပါတယ်

1887-1954 ကာလအတွင်းမှာတော့ သွေးအမျိုးအစားအုပ်စုခွဲကာ စစ်ဆေးခြင်း ပညာရပ်ဟာ ထွန်းကားလာပါတယ်

1891-1955 သေနည်ကျည်ဆံကို ကြည့်ပြီး အမျိုးအစားခွဲခြားတဲ့ ပညာရပ်တိုးတက်လာပါတယ် ...

1932 FBI ကနေ နည်းပညာရှင်နဲ့ Agent ပေါင်း 500 ကျော်နဲ့ အထက်ဖော်ပြစစ်ဆေးမှုတွေပြုလုပ်ဖို့ အတွက် Forensics LAB ကိုတည်ထောင်ခဲ့ပါ တယ်

1984 FBI ကို ကူညီရန် The Computer Analysis and Response Team (CART)ကို စတင်ထည်ထောင်ခဲ့ပါတယ် ...

1993 Computer သက်သေခံချက်တွေအတွက် ပထမဆုံး Conference ကို အမေရိကန်နိုင်ငံမှာ ကျင်းပခဲ့ပါတယ် ...

1995နည်းပညာဖလှယ်ရန် International Organization on Computer Evidence (IOCE) ကိုတည်ထောင်ခဲ့ပါသည်။

1998The International Forensic Science Symposium ကို Computer Forensics နှင့်ပတ်သတ်သော သတင်းအချက်အလက်တွေ ဖလှယ်ရန် တည်ထောင်ခဲ့ပါတယ် ...

2000ပထမဆုံး FBI Regional Computer Forensic Laboratory (RCFL) ကိုတည်ထောင်ခဲ့ပြီး Digital သက်သေခံချက်တွေကို ဖော်ထုတ်ခဲ့ပါတယ် ..

Cyber Crime တစ်ခုကို ဆက်စပ်စဉ်းစားရန်မှာ ... Cyber or electronic Law မှာပြဌာန်းထားတာ ပါမပါ ကြည့်ရပါမယ် ဆက်စပ်မှုရှိ မရှိ လေ့လာရပါမယ်

ဥပမာ ... bank တစ်ခုက... Bank website ကနေ ယနေ့ us ဒေါ်လာ ဈေးကို 1500 နဲ့ကျောင်းမယ် တစ်ခြားbankတစ်ခုက1300ရောင်းဈေး...ဒီ Case မှာဆိုရင် Ethic မရှိတာကိုပဲ တွေ့ရမယ် ... webiste ပေါ်ကနေဖြစ်ပေမဲ့ Cyber Crime case မဖြစ်ဘူး

နောက်တစ်ခုကကျယ်ကျယ်ပြန့်ပြန့်သက်သေခံနိုင်လုံအောင်ယူမဲ့အပိုင်း...ဥပမာ... ကလေးလိင် အကြမ်းဖက် ပုံတွေတင်တဲ့သူကို စစ်မယ် သူ့ Device ထဲကနေ ပုံတစ်ပုံပဲတွေ့တယ် ... ဒီလောကကနဲ့ တရားရုံးမှာ တင်ပြရင် သက်သေမခံနိုင်လုံဘူးနောက်တစ်မျိုးက DDOS Attack တိုက်နေတယ်လို့ယူဆရတဲ့ Device တစ်ခု....တရားခံဟာ .CNC ပြုလုပ်ပြီး .တစ်ကယ် တိုက်နေတာလဲဖြစ်မယ်.ဒါမှမဟုတ် ... မသိလိုက်ဘဲ DDOS တိုက်ဖို့ Bot တစ်ခု (အလွယ်ကူဆုံးဆိုရင် Device မှာ virus (ဝင်နေတာ) လဲဖြစ်နိုင်တယ် အဲဒါမျိုးဆို တစ်ဖက် ရှေ့နေ ဘက်က ခြေပိုင်ရင် လွတ်ဖို့သေချာသလိုက်ရှိနိုင်တယ် ...

ဒါကြောင့် သံသယရှိယုံထက် သက်သေကို ခိုင်ခိုင်မာမာပြနိုင်ရမယ် ...

Forensics စစ်ဆေးမဲ့သူတစ်ယောက်ရဲ့ ရှိရမဲ့ IT နဲ့ပတ်သတ်တဲ့ Knowledge ကို part 4 မှာရေးထားပြီးပါပြီ....

IT Knowledge အပြင်နောက်ထပ်ရှိရမယ့် အရည်အချင်းတွေကတော့ ...

- နောက်ကြောင်းရာဇဝင်ရှင်းရပါမယ်
- IT နဲ့ပတ်သတ်တဲ့ Degree တစ်ခုရထားနိုင်ရင်ပိုကောင်းပါတယ်
- Forensicsစစ်ဆေးဖို့ ကောင်းကောင်းလေ့ကျင့်ထားတဲ့သူဖြစ်ရပါမယ်
(တရားရုံးမှာသက်သေထွက်ခြင်း...အသုံးပြုတဲ့ForensicsLabကို ကျွမ်းကျင်စွာအသုံးပြုနိုင်ခြင်း)
- ITနဲ့ပတ်သတ်တဲ့အပိုင်းမှာအတွေ့အကြုံရှိရပါမယ် .

- (၁) A++
- (၂) Operationsystem(window,linux,MAC,etc..)
- (၃) BasicNetworking
- (၄) RoutingandSwitching
- (၄) ProgrammingBasic
- (၅) Server/Vmware/Bigdata -Virusမျိုးစုံသဘောတရား
- (၆) Webapplication
- (၇) SocialNetwork(Facebook,twitter,linkedin,etc....)
- (၈) Mobilephone..Tablet(software,hardware)
- (၉) wirelessDevice..

အဲထဲက တစ်ခုထက်ပိုရပါမယ်

- တရားခွင်မှာလိုအပ်ပါက....မိမိအမှုအတွက်ITပိုင်းဆိုင်ရာကူညီသက်သေထွက်ဆိုပေးမဲ့သူကို ရွေးတတ် ရပါမယ်.....
- ITပိုင်းဆိုင်ရာCertificationသို့Forensics ဆိုင်ရာ Certificationရရှိထားရပါမယ် .
- အစိုးရရှေ့နေမှလွဲပြီးကျန်ရှေ့နေတွေနဲ့ထဲထဲဝင်ဝင်ပတ်သတ်မှုကင်းရပါ မယ်။ ပါတီ အဖွဲ့အစည်း တွေနဲ့ ပတ်သတ်မှုကင်းရပါမယ်။
- ပြေပြစ်စွာ ဆက်ဆံပြောဆိုတတ်သူဖြစ်ရပါမယ်။

How to Management Evidence ?

ပထမဆုံးမူရင်းဖြစ်ပွားနေရာရောက်မယ်... - မူရင်းနဲ့ဆက်စပ်နေတဲ့ Device အားလုံးကို သိမ်းဆည်းမယ်...သိမ်းဆည်း ရမဲ့ နည်းလမ်းအချို့ကို အရင်ဆောင်းပါးတွေမှာရေးသားထားပါတယ်

သိမ်းဆည်းပြီးရင် Deviceတွေကိုစာရင်းလုပ်မယ်...ဘယ်နေရာကသိမ်းတာလဲ.. Case ကဘာလဲ

....

ဖမ်းဆီးတဲ့အချိန်မှာ deviceက Power On နေလား Off နေလား ။ Deviceက ပျက်စီးနေပြီလား။

Deviceနဲ့ဘာတွေချိတ်ဆက်ထားလဲ...phone Printer USB HD Modem Wireless AP , LAN cable ...etc.....Deviceအမျိုးအစား..

- ချိတ်ဆက်နေတဲ့အနေအထားအတိုင်း View ပေါင်းစုံကနေ photo သို့ video ရိုက်မယ် ... ဖြုတ်သိမ်းပြီးမှရိုက်ရင်တရားရုံးမှာအငြင်းပွားလာစရာတွေရှိနိုင်တယ်

ဥပမာ-ပုံစံကိုပုံတွေမှာဖော်ပြထားပါတယ်....ပထမပုံမှာဆိုရင် laptop နဲ့ External HD နဲ့ချိတ်ဆက် ထားတယ်... အပေါ်မှာပြောသလိုတပ်ဆင်ထားတဲ့အတိုင်းပဲ ဓာတ်ပုံရိုက်မယ် ...ဒုတိယပုံမှာ ဆိုရင်... Printer Monitor KeyBoard ပုံတွေရပါမယ် ...photo ရိုက်မယ် ပြီးရင် ... ဆက်ဆစ်စဉ်စားရမဲ့

အပိုင်းက Printerနဲ့ဘာတွေထုတ်ထားသလဲ.....ထုတ်ပြီးသားစာရွက် စာတမ်း တွေရှိသလား ရှာဖွေရမယ်...အမှိုက်ပုံထဲကအစရှာဖွေ ရမယ် ... dumpster dumping ဝေါ့Monitor KeyBoard ရှိနေတဲ့အတွက် နောက်ထပ် ကွန်ပျူတာ တစ်လုံးရှိနေသေးသလား ...ဆိုတာပါ စဉ်းစားရမယ်

နောက်ထပ်ရေးမဲ့အပိုင်းကတော့ evidence သယ်ယူမဲ့အပိုင်းနဲ့ ... ဘယ်လို မပျက်စီးအောင် ကာကွယ်ရမဲ့ အပိုင်းဖြစ်ပါတယ်

FORC



သက်သေခံ Device အားမပျက်စီးအောင် ကာကွယ်ခြင်း

သက်သေခံသိမ်းဆည်းပုံ ... မှတ်တမ်းယူပုံ...တို့ကို အရင် post တွေမှာတင်ခဲ့ပြီးပါပြီ.... အခု ရေးသားမှာက သက်သေခံ Device အားမပျက်စီးအောင် ကာကွယ်ခြင်း အပိုင်းဖြစ်ပါတယ်

သိမ်းဆည်းရမိတဲ့ Device ကိုစစ်ဆေးတဲ့အချိန်မှာ အမှားအယွင်းရှိခဲ့ရင် ပြန်လည်စစ်ဆေး လို့ရနိုင်အောင် Device ကို Clone (ထပ်တူ ကူးယူ) ရပါမယ်.... Linux မှာလဲ clone ယူနိုင်သလို forensics tools တွေဖြစ်တဲ့ Encase, Access Data tools တွေနဲ့လဲ clone ယူနိုင်ပါတယ် ... Original image ရဲ့ Hash Value (MD5 သို့ SHA1) နဲ့ Clone image ရဲ့ hash value တူရပါမယ် Example soon

device ကို clone မယူခင်မှာ Write Protect (read only) စနစ်ဖြစ်အောင်ပြုလုပ်ရပါမယ် Data တွေကို မူရင်း device မှာထပ်ပြီးပြင်ဆင်လို့ မရနိုင်အောင်ဖြစ်ပါတယ်case အမျိုးအစား write protect ပြုလုပ်သူ ပြုလုပ်တဲ့နေ့စွဲ device အမျိုးအစားတို့ကို မှတ်တမ်းထားရှိရပါမယ်... Linux သို့ forensics tool, controller တွေမှာ write protect ပါဝင်ပါတယ် ... Example

....Soonထပ်ပြီးကာကွယ်ရမဲ့အပိုင်းကတော့ သက်သေခံ Device ကို စစ်ဆေးမဲ့နေရာကို သယ်ဆောင်နေစဉ် (သို့) စစ်ဆေးရန်သိမ်းထားနေစဉ်အတွင်း (သို့) စစ်ဆေးပြီး တရားရုံးသို့ မတင်မှီကာလအတွင်းမှာ အီလက်ထရောနစ် လှိုင်းတွေရဲ့ နောက်ယှက်မှုမှ ကင်းဝေးအောင် Remote လုပ်ပြီး data တွေပျက်စီးစေခြင်းမှ(wipe လုပ်ခြင်းမှ) ကာကွယ်နိုင်အောင် ပြုလုပ်ရပါမယ်။

(အချို့သောဖုန်းများတွင် ဖုန်းအခိုးခံရပါက phone data တွေကို wipe လုပ်တဲ့ အပိုင်းပါဝင်နေပါတယ်) (spyware ထည့်ထားရင်လဲ wipe လုပ်နိုင်ပါတယ် ...) ဒါ့ကြောင့် EMI နဲ့ EFI ကိုခံနိုင်တဲ့အထူးပြုလုပ်ထားတဲ့ အိတ်တွေ .. ဗီဒီယိုတွေ အခန်းတွေနဲ့သိမ်းဆည်းရမှာဖြစ်ပါတယ်

နောက်တစ်ခုကတော့ worm storage စနစ်ဖြစ်ပါတယ် ... (Write One Read many) ကိုဆိုလိုပါတယ်။ file တစ်ခုကို save လိုက်တာနဲ့ save လိုက်တဲ့ file ကို ချက်ခြင်း write protect ဖြစ်စေပါတယ်...နောက်ထပ်ရေးမဲ့အပိုင်းကတော့ evidence သယ်ယူမဲ့အပိုင်း ဖြစ်ပါတယ်

သက်သေခံ Device အားမပျက်စီးအောင် ကာကွယ်ခြင်း

သိမ်းဆည်းရမိတဲ့ Device ကိုစစ်ဆေးတဲ့အချိန်မှာ အမှားအယွင်းရှိခဲ့ရင် ပြန်လည်စစ်ဆေး လို့ရနိုင်အောင် Device ကို Clone (ထပ်တူ ကူးယူ) ရပါမယ်.... Linux မှာလဲ clone ယူနိုင်သလို forensics tools တွေဖြစ်တဲ့ Encase, Access Data tools တွေနဲ့လဲ clone ယူနိုင်ပါတယ် ... Original image ရဲ့ Hash Value (MD5 သို့ SHA1) နဲ့ Clone image ရဲ့ hash value တူရပါမယ် device ကို clone မယူခင်မှာ Write Protect (read only) စနစ်ဖြစ်အောင်ပြုလုပ်ရပါမယ် Data တွေကို မူရင်း device မှာထပ်ပြီးပြင်ဆင်လို့ မရနိုင်အောင်ဖြစ်ပါတယ်case အမျိုးအစား write protect ပြုလုပ်သူ ပြုလုပ်တဲ့နေ့စွဲ device အမျိုးအစားတို့ကို မှတ်တမ်းထားရှိရပါမယ်... Linux သို့ forensics tool, controller တွေမှာ write protect ပါဝင်ပါတယ် ...

ထပ်ပြီးကာကွယ်ရမဲ့အပိုင်းကတော့ သက်သေခံ Device ကို စစ်ဆေးမဲ့နေရာကို သယ်ဆောင် နေစဉ် (သို့) စစ်ဆေးရန်သိမ်းထားနေစဉ်အတွင်း (သို့) စစ်ဆေးပြီး တရားရုံးသို့ မတင်မှီကာလ အတွင်းမှာ အီလက်ထရောနစ် လှိုင်းတွေရဲ့ နောက်ယှက်မှုမှ ကင်းဝေးအောင်

Remote လုပ်ပြီး data တွေပျက်စီးစေခြင်းမှ(wipe လုပ်ခြင်းမှ) ကာကွယ်နိုင်အောင် ပြုလုပ်ရပါမယ်။

(အချို့သောဖုန်းများတွင် ဖုန်းအစိုးခံရပါက phone data တွေကို wipe လုပ်တဲ့အပိုင်း ပါဝင် နေပါတယ်) (spyware ထည့်ထားရင်လဲ wipe လုပ်နိုင်ပါတယ် ...) ဒါ့ကြောင့် EMI နဲ့ EFI ကိုခံနိုင်တဲ့ အထူးပြုလုပ်ထားတဲ့ အိတ်တွေ .. ဗီဒီယိုတွေ အခန်းတွေနဲ့ သိမ်းဆည်းရမှာဖြစ်ပါတယ် ..



နောက်တစ်ခုကတော့ worm storage စနစ်ဖြစ်ပါတယ် ... (Write One Read many) ကိုဆိုလိုပါတယ်။

file တစ်ခုကို save လိုက်တာနဲ့ save လိုက်တဲ့ file ကို ချက်ခြင်း write protect ဖြစ်စေပါတယ်။

သက်သေခံ ပစ္စည်းအားပို့ဆောင်ခြင်း...

မူရင်းဖြစ်ပွားရာနေရာကနေ Forensics lab ကိုပို့ဆောင်တဲ့နေရာမှာ အချိန်အကန့် အသတ် ထားရှိရပါမယ် .. ဘာကြောင့်လဲဆိုတော့ ... digital သက်သေခံပစ္စည်းများကို မသမာသူ နည်းပညာကျွမ်းကျင်သူက ကြားဖြတ်ပြီး ဖြတ်ဆီးနိုင် ပြင်ဆင်နိုင်လို့ပါ eg ... Wipe Data ... file , folder. date တွေရဲ့Modified date ကိုပြောင်းလဲခြင်း

CSI ဇာတ်ကားထဲမှာပါတာကို ဥပမာပြရရင် သက်သေခံပစ္စည်းသယ်ဆောင်သွားသူက သတ်မှတ်ချိန်ထက်နောက်ကြပြီးမှ forensics lab ကိုရောက်သွားပါတယ် ..အဲဒါကို တစ်ဖက်က ရှေ့နေက သိသွားပြီး ... သက်သေခံ device ကို တရားရုံးမှာ တင်ပြခြင်းကို ကန့်ကွက်ပါတယ် နောက်ကျတဲ့ အကြောင်းကို ခိုင်မာတဲ့ အချက်အလက်လဲမပြနိုင်တဲ့အခါမှာ တရားသူကြီးက သက်သေခံသွင်းတာကို ပယ်ချပါတယ် (CSI ဇာတ်ကားထဲမှာနော် 😊:)

forensics lab ကျောက်လင်စစ်ဆေးသူ ... စစ်ဆေးတဲ့နေ့ရက် အချိန် ... အမှု
ဘာကိုအသုံးပြုပြီးစစ်ဆေးသလဲဆိုတာကို record လုပ်ထားရပါမယ် paper အစား evidence
tracking software , barcode , RFID တို့နဲ့လဲ မှတ်တမ်းယူနိုင်ပါတယ်

သက်သေခံပစ္စည်းကိုလဲ မသက်ဆိုင်သူများ မကိုင်တွယ်နိုင်စေရန် physical Security
ကိုချမှတ်ထားရပါမယ်

စစ်ဆေးပြီးနောက် သက်သေခံ device ကို ထားသိုခြင်း

မီးလောင်လွယ်တဲ့နေရာ မီးခိုးထွက်ခြင်း ,ပူလွန်း အေးလွန်းခြင်း ရေယိုခြင်း EMI
ကြောင့်ထိခိုက်မှုမရှိတဲ့နေရာဖြစ်ရပါမယ်

ISO သတ်မှတ်ချက်အရ Data evidence သိမ်းဆည်းမဲ့ အခန်း Class 100 , Class 150 , Class
350 ရှိရပါမယ်မီးဘေးအတွက် Class A,B,C,D,E အဆင့်တွေရှိပါတယ်

အမေရိကန်တပ်မတော်မှ evidence device သိမ်းဆည်းရာတွင် လိုက်နာရမဲ့ အချက်တွေကို
သတ်မှတ်ထားပါတယ်

၁။ အပူချိန်မြင့်ခြင်း နိမ့်ခြင်းမရှိသောနေရာ ဖုန်မရှိသောနေရာများတွင် သိမ်းဆည်းရပါမယ် ..

၂။ EMI နောက်ယှက်မှုကင်းသောနေရာဖြစ်ရပါမယ်..

၃။ evidence ပစ္စည်းတွေကို ရောနှောထားခြင်း မရှိရပါဘူး ...

၄။ ပါဝါသွင်းထားဖို့ လိုအပ်တဲ့ device တွေကို ပါဝါသွင်းထားရပါမယ် ...

၅။ မီးလောင်လွယ်တဲ့နေရာမှာ မထားရှိရပါဘူး အပူချိန် 120 F ထက် ကျော်လွန်ခြင်းမရှိရပါ

၆။ အလိုအလျှောက် မီးငြိမ်းတဲ့ ပိုက်တွေနဲ့နီးရာမှာမထားရှိရပါဘူး
ထားရှိရင်လဲရေမဝင်အောင်ထားရှိရပါမယ် ...

၇။ Chemical ပစ္စည်းတွေနဲ့ ရောနှောမထားရှိရပါ

Anti-DigitalForensics

Digital Evidence စစ်ဆေးရာတွင်တွေ့နိုင်သော အခက်အခဲများ

Digital Evidence ဆိုသည်မှာ Digital ပုံစံဖြင့် မည်သည့်သတင်းအချက်အလက်မဆို သိမ်းဆည်းထားသည်ဖြစ်စေ ... ဆက်သွယ်နေသည်ဖြစ်စေ သက်သေထင်ရှားစွာပြနိုင်သော အရာကို ခေါ်ဆိုပါသည်။

Digital Evidence သည် ပျက်စီးလွယ်ခြင်း ကျွမ်းကျင်သူမှ ပုံဖျက်နိုင်ခြင်းတို့ကြောင့် စစ်ဆေးရာတွင် အခက်အခဲဖြစ်ခြင်း ... အချိန်ကြာစေခြင်းတို့ဖြစ်စေနိုင်ပါသည်... ။

သိမ်းဆည်းနေစဉ် device ကိုပါဝါရုတ်တရပ်ပိတ်လိုက်ခြင်း (Ram ပေါ်တွင် လုပ်ကိုင်နေသာ အလုပ်များ ပျက်စီးစေနိုင်ပါသည်။

- storage ကို ဖျက်ဆီးခြင်း (example . Format အကြိမ်များစွာချခြင်း;)

- အရေးကြီးသော အချက်အလက်များကို ဓာတ်ပုံများ ဖိုင်များအတွင်းရောထည့်ထားခြင်း

- file or data များအား Password ခတ်ခဲစွာပေးပြီး သိမ်းထားခြင်း (ဥပမာ rar သို့ zip ပြုလုပ်ပြီး password ပေးထားခြင်း)

- Bootable Cd /DVD /stick များကြောင့် စစ်ဆေးရန် အခက်တွေ့ခြင်း

- စစ်ဆေးသူမှ နည်းပညာကျွမ်းကျင်မှု နည်းခြင်း သက်ဆိုင်ရာ အပိုင်းလိုက် ကျွမ်းကျင်သူ နည်းပါးခြင်း

- စစ်ဆေးရာတွင် အသုံးပြုသော device / software များ အားနည်းချက်ရှိခြင်း

Type of Digital Data (Digital Data အမျိုးအစားများ)

Volatile Data

(ပျက်စီးလွယ်သော Data သို့မဟုတ် ပြင်ဆင်နိုင်သော Data) Ram (primary memory) ပေါ်မှာ အလုပ်လုပ်နေတဲ့ အလုပ်တွေဖြစ်ပြီး Power Off ဖြစ်တာနဲ့ ပျောက်ကွယ်သွား ပျက်စီးသွား မှာဖြစ်ပါတယ်...(ပြင်ဆင်လို့လဲရပါတယ်) user log on , Process information, command history, network history စသည့်တို့ဖြစ်ပါတယ်

Ram ပေါ်မှာ အလုပ်လုပ်တဲ့ bootable CD DVD stick တို့နဲ့ Privacy ချိုးဖောက်မယ် ဆိုရင် ..
forensics လုပ်သူအနေနဲ့ အခြားသက်သေကို ရှာဖွေရမှာဖြစ်ပါတယ်

Non-VolatileData (မပျက်စီးလွယ်သောData)

Volatile information က ကွန်ပျူတာ ပါဝါမရှိတာနဲ့ ပျောက်ပျက်သွားပြီး
Non-Volatile Data ကတော့ ပါဝါမရှိလဲ အချက်အလက်တွေ တည်ရှိနေပါမယ် ဒါဆိုရင်
ကွန်ပျူတာရဲ့ Secondary Storage ဖြစ်တဲ့ Hard disk မှာသိမ်းဆည်းထားတဲ့ data
တွေဖြစ်ပါတယ် hidden file , Swap file. index.dat file , Registry file. event log
စတာတွေဖြစ်ပါတယ်

TransientData (မတည်မြဲပျောက်ကွယ်သွားမည့်Data)

ဥပမာ website တစ်ခုကို ဖွင့်နေရင်းနဲ့ မီးပျက်သွားသည်ဖြစ်စေ
မဖွင့်ချင်ရင်ဖြစ်စေ ပိတ်လိုက်တာမျိုး Application တစ်ခုကို သုံးနေရင်း နဲ့ ရုတ်တရက်
အကြောင်းတစ်ခုကြောင့်ပိတ်သွားတာမျိုး ..အလွယ်ဆုံးပြောရရင် ... ကွန်ပျူတာ
ပါဝါဖွင့်ထားနေဆဲမှာပဲရှိနေတဲ့Dataမျိုးပါ။

example Active Network Connection

FragileData (ပျက်စီးနိုင်သည့်Data)

Hard Disk , Memory Stick , CD , DVD တို့မှာ သိမ်းထားတဲ့ Data တွေဖြစ်ပါတယ်
ပြောင်းလဲနိုင် ပြင်ဆင်နိုင် ပျက်စီးနိုင်ပါတယ် ...Example , File တစ်ခုကို ဖွင့်တဲ့နေ့ ...
ပြင်တဲ့နေ့.

TemporarilyAccessData

HardDisk,MemoryStick,CD,DVDတို့မှာသိမ်းထားတဲ့Data,Encrypted file system တို့ပါနိုင်
ပါတယ်။

ActiveData

Computer power ဖွင့်နေတုန်း ဆက်စပ်လုပ်ကိုင်နေတဲ့ အလုပ်များဖြစ်ပါတယ် ...

ArchivalData

rar , zip , tar (linux) , iso စသည်ဖြင့်ဖြစ်ပါတယ် ..

BackupData

ကွန်ပျူတာ(သို့မဟုတ်)DatabaseကိုBackupလုပ်ထားတဲ့Data များဖြစ်ပါတယ် HD

တစ်ခုထဲမှာ သို့မဟုတ် အခြားမှာဖြစ်စေရှိနိုင်ပါသည်။အပေါ်မှာ ရေးထားတဲ့ အချက်တွေအရ Ram ကိုစစ်ဆေးတဲ့ နည်းပညာပိုင်းကို အထူးသဖြင့်လေ့လာရမှာဖြစ်ပါတယ်

Collection Evidence

တွေ့နိုင်တဲ့ evidence file နေရာတွေကတော့ Server,Ram.Hard disk , CD DVD, removable storage , cartridges စတဲ့နေရာတွေပဲဖြစ်ပါတယ်.....

User Created File

User ပြုလုပ်ထားတဲ့ အရာအားလုံးဖြစ်ပါတယ် ... example= database file , documents file , audio video file, text file , internet bookmarks,

User Protected File

အသုံးပြုသူက အခြားသူမမြင်စေရန် ကာကွယ်ထားတဲ့ File များ ဖြစ်ပါတယ်... Example password protect file , folder , hidden file , rar,zip, tar,

Computer Created File

စနစ်မှ အလိုအလျောက် ပြုလုပ်ထားတဲ့ File တွေဖြစ်ပါတယ် example = backup file , server log, event logs , system file , swap file, printer pools

Electronic Device တွေကတော့ နေ့စဉ် ပတ်ဝန်းကျင်မှာ အသုံးပြုနေတဲ့ smart card တွေ အပါအဝင် ကျန်တဲ့ device တွေပဲဖြစ်ပါတယ် ...အရှည်တော့မရေးတော့ပါဘူး ပုံမှာလဲဖော်ပြထားပါတယ်။ကျန်တဲ့အပိုင်းကတော့ အထက်က နေရာတွေကနေ evidence ကိုရှာဖွေရန်ဖြစ်ပြီး.. .အခြေအနေ , evidence Seizing အလိုက် power on သင့် မသင့်နဲ့ .Device ကို bit by bit copy ယူခြင်း တို့ဖြစ်ပါတယ် ။

ဖွင့်ထားတဲ့ သက်သေခံ Computer ကနေ သက်သေခံများရှာဖွေခြင်း

Running Process (ဘာ Process တွေ Run နေလဲ)Network Status (wireless နဲ့လား ဘာနဲ့အသုံးပြုနေသလဲ) VPN အသုံးပြုထားသလား Proxy ကျော်ထားလား ...Opening File (ဘာဖိုင်တွေဖွင့်ထားသလဲ)Browser နဲ့ ဘာတွေ ဖွင့်ထားသလဲ ...Printer နဲ့ ဆက်ထားရင် Print Pool နဲ့ ထုတ်ထားတဲ့ စာရွက်တွေကို ရှာဖွေပါမယ် ...ကိုယ့်သဘောနဲ့ကို ဘာဖိုင်မှ လျှောက်မဖွင့်ရပါဖွင့်ထားသမျှeventlogကျန်နေတတ်ပါသည်...ကွန်ပျူတာနဲ့ ချိတ်ဆက်ထားသမျှကို ဓါတ်ပုံ မှတ်တမ်း ယူပါမယ် ..Router တွေ Switch တွေ ပါနေရင်

ချိတ်ဆက်ထားတဲ့

Port

တွေကို

ဝတ်ပုံမှတ်တမ်းယူပါပိတ်နေတဲ့ ကွန်ပျူတာတွေ Device တွေကို ပါဝါ မဖွင့်ရပါ..ကွန်ပျူတာ ပွင့်နေဆဲဖြစ်ရင် Screen ပေါ်ရှိသမျှကို ကို ဝတ်ပုံမှတ်တမ်းယူပါScreen Saver ဖြစ်နေရင် ... ပြန်ပွင့်အောင် Mouse ကို ဖြည်းဖြည်းရွှေ့ပါ... Screen Saver ကနေ login Password တောင်းတဲ့အနေအထားကို ရောက်ရင် .. ဝတ်ပုံမှတ်တမ်းယူထားပါ dont make anythings ကွန်ပျူတာနဲ့ ချိတ်ဆက်ထားသမျှကို ဖြုတ်သိမ်းပါ (example ..usb, router , modern)

Electronic Crimeတစ်ခုချင်းစီတွင်ပတ်သတ်ဆက်နွယ်နေသောသက်သေခံချက်များ

Onlineလေလံများနှင့်လိမ်လည်မှုများ...

-ငွေကြေးစာရင်းများ(eg..database,excel,paper),-online တွင် အသုံးပြုသော Account websiteaddress book , account software,ငွေစာရင်းအမှတ် Credit card ..internet Browser historyphone call log, mesage logemail, note , social network chat log ,Photo, Screenshootလိင်မှုကိစ္စအနိုင်ကျင့်မှုများ ..Image, video , social chat log,internet activities, browser activities,phone content , call log ,ငွေစာရင်းအမှတ် Credit card .

Computer မှတစ်ဆင့် ကျူးလွန်မှုများconfiguration file, exe file, bat file, rar, zip, tar,.... internet activities, Browser log ,text file, email log, social log , source code,ip address and Mac address,ငွေစာရင်းအမှတ် Credit cardအခြားသောမူရင်းများဖြစ်သည့် အွန်လိုင်းလောင်းကစားငွေအကျပ်ကိုင်တောင်းဆိုမှု မဲလိမ်လည်မှုတို့.ရှိသက်သေခံချက်များသည် အထက်ပါအချက်များနှင့် များစွာဆင်တူပါသည်

(Internet of things (IoT) devic များမှလည်း ကျူးလွန်နိုင်ကြောင်းသတိပြုသင့်ပါသည်.....

Identity Theft (ID ခိုးယူခြင်း)

Creditcareအလွတ်များ

CreditCardReaderနှင့်Writer

CreditcardGenerator

Credit Card No များ ... Text file သို့ မဟုတ် rar Zip ဖိုင်များဖြင့်ထည့်ထားတတ်သည်...

ပြည့်တန်ဆာအမှု

ငွေကြေးစာရင်းလူစာရင်း(excel,world,database)

ဆေးစစ်စာရင်း

Imagefile

Email,Note,Letterbrowser,chatrecord,

Content No , call log

မူးယစ်ဆေးဝါးအမှု

ငွေကြေးစာရင်း(excel,world,database)

Imagefile

Email,Note,Letterbrowser,chatrecord,

Content No , call log

ဆက်သွယ်ရေးချိုးဖောက်မှု

SimcardClone(hardware)

userdatabase ElectronicSerialnumber(ESI)

MobileidentificationNumber(MIN)

Browser,socialNetworkRecord

Steganography

Steganography ဆိုတာ မြင်သာတဲ့ အရာဝတ္ထုထဲကို ကိုယ်ပုဂ္ဂိုလ်ထားချင်တဲ့ အရာကို ပေါင်းထည့်ထားခြင်းဖြစ်ပါတယ် ...မြင်သာအောင်ပြောရရင် ... ငယ်ငယ်တုန်းက ကောင်မလေးကို ရည်းစားစာပေးချင်တယ်သိမှာလဲကြောက်တယ်အဲတော့စာအုပ်ငှားသလိုလိုနဲ့ရည်းစားစာကိုစာအုပ်ထဲမှာစာညှပ်ပေးတယ်.....ဒီသဘောပါပဲ.Steganography ဆိုတာဂရိ ဘာသာစကား ကနေလာတာဖြစ်ပြီးဂရိတွေကစတင်အသုံးပြုခဲ့ပါတယ်။ တရုတ်တွေ မွန်ဂိုလက်အောက် ရောက်တုန်း ကလဲသုံးခဲ့ပါတယ်...အမေရိကန်ပြည်တွင်းစစ် ပထမကမ္ဘာစစ်ဒုတိယကမ္ဘာစစ် အတွင်းမှာလဲအသုံးပြုခဲ့ပါတယ်။

လက်ရှိမှာအသုံးပြုနေတာတွေကတော့

-virusဖြန့်ခြင်း...

-ဥပဒေနဲ့မညီတဲ့Messageတွေပို့တဲ့အချိန်..

-Spyတွေအချင်ချင်းMessageပို့တဲ့အချိန်..

-Hackingပြုလုပ်ရန်ရည်ရွယ်ချက်..

- လျှို့ဝှက်ချက်ကို မသိအောင် သိမ်းရန် စသည်ဖြင့်ရှိပါတယ်..

PHOTOအတွင်းထည့်သွင်းခြင်း

MP3အတွင်းထည့်သွင်းခြင်း

VIDEOFILEအတွင်းထည့်သွင်းခြင်း

DOCUMENTSFILEတွေအတွင်းထည့်သွင်းခြင်း

FOLDERအတွင်းထည့်သွင်းခြင်း

SPACETABတွေအကြားအတွင်းထည့်သွင်းခြင်း

Websiteအတွင်းထည့်သွင်းခြင်း(Forensicsပြုလုပ်ရန်ခက်ခဲ)

Emailအတွင်းထည့်သွင်းခြင်း(spammailအဖြစ်)

DVD/CDအတွင်းထည့်သွင်းခြင်း

programmingcodeအတွင်းထည့်သွင်းခြင်း

OSအတွင်းထည့်သွင်းခြင်း

Text file အတွင်းထည့်သွင်းခြင်း

စသည်ဖြင့်အမျိုးမျိုးရှိပါတယ်...

တစ်ခုစီကိုရေးရမှာဖြစ်တဲ့အတွက်နည်းနည်းတော့ရှည်ပါမယ်... စစ်ဆေးပုံနည်လမ်း ကလဲ

အမျိုးမျိုး ရှိပါတယ်။

ခါတ်ပုံအတွင်း Secret ထည့်သွင်းခြင်း

jPEG,JPG,PNG,BMP စတဲ့ ဖော်ပုံတွေမှာ မိမိပုဂ္ဂိုလ်ချင်းတွဲ စာသားကို ထည့်ပြီး အများမသိအောင်

ပုဂ္ဂိုလ်ထားခြင်းပါ...ပုဂ္ဂိုလ်တို့နည်းစနစ်ကတော့ ဖော်ပုံရဲ့ Pixel နဲ့ Resolution

အနေအထားကိုလိုက်ပြီး bit တွေကို တစ်နေရာခြင်းစီအလိုက်အစားထိုးတာပါ ...တစ်နေရာခြင်းစီ

အလိုက်အစားထိုးလိုက်တဲ့အတွက်အများအမြင်မှာမသိသာတော့ပါ။Eg.....ပုံရဲ့ bitstream

ကအောက်ပါအတိုင်းဆိုပါစို့...

(10111110) (10111111) (10111111) (10111111) (10111111) (10111111)
(10111111) (10111110)

အဲဒါအထဲမှာ A ဆိုတာထည့်ပွက်မယ် ဆိုရင် A ရဲ့ binary က 10000001 ဖြစ်ပါတယ်။ ထည့်ပွက်တဲ့ ပြီးတဲ့ အချိန်မှာ ပုံရဲ့ bit stream က အောက်ပါအတိုင်း ပြောင်းလဲသွားပါမယ်နောက်ဆုံးအလုံးတွေကို ကြည့်ကြည့်ပါ..

(10111111) (10111110) (10111110) (10111110) (10111110) (10111110)
(10111110) (10111111)

အထက်ပါနည်းကို Least bit Intersection (LSB) လို့ခေါ်ပါတယ်။

mp3 ဖိုင်များအတွင်းထည့်သွင်းခြင်း

mp3 .wav ဖိုင်များအတွင်း မိမိပွက်ချင်တဲ့ စာသား သို့မဟုတ် စကား ကို ထည့်ပြီး အများမသိအောင် ပွက်ထားခြင်းပါ...ပွက်တဲ့နည်းစနစ်ကတော့ အထက်မှာဖော်ပြထားတဲ့ Least bit Intersection (LSB) နည်းစနစ် Frequency (DSSS-Direct Sequence Spread Spectrum) (FHSS-FrequencyHoppingSpreadSpectrum)(ECHO) နည်းစနစ်တို့ဖြစ်ပါတယ် .. ။

Least bit Intersection (LSB) စနစ်ကိုတော့ အထက်မှာဖော်ပြထားပြီးဖြစ်ပါတယ် ..

E-mail Forensics

Type Of Crime E-mail

malware ဖြန့်ရန် အတွက်အသုံးပြုခြင်း Spam Mail (ကြော်ငြာအဖြစ်လဲတွေ့ကရတတ်သည်)

အနိုင်ကျင့် အကျပ်ကိုင်ရန် အတွက်အသုံးပြုခြင်း (Cyber Stalking)

လိမ်လည်ရန်အတွက် အသုံးပြုခြင်း (Fraud Mail)

မိမိလိုလားချက်ရရှိအောင်တစ်ဖက်လူအားဆွဲဆောင်ခြင်း(phishing)

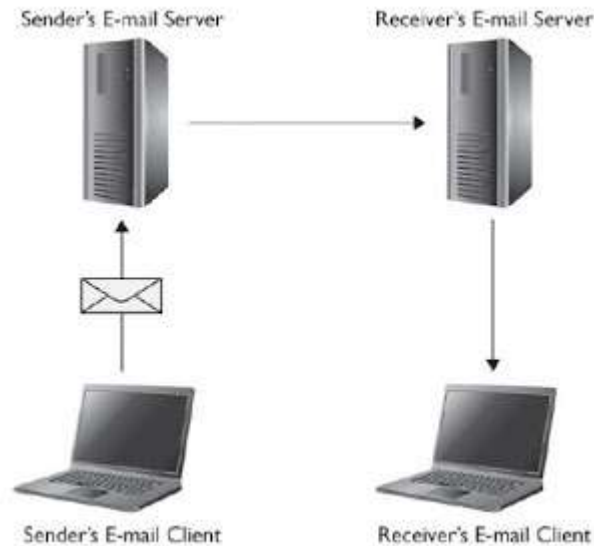
(Email မှာတင်မက telephone message ဖြင့်လဲဆွဲဆောင်တတ်သည်)

မိမိလိုလားချက်ရရှိအောင် တစ်ဖက်လူအားဆွဲဆောင်ခြင်း (phishing) အမျိုးအစားများ -----

- မက်လုံးဖြင့် မြူဆွယ်ခြင်း (ဥပမာ ဖုန်းကို လျှော့ဈေးဖြင့်ပေးမယ်)

- ကြောက်စိတ် ကို အသုံးပြုပြီး မြို့ဆွယ်ခြင်း (Bank Security အရ သင့် account password ကိုချက်ချင်းချိန်းပါ) (လက်တလော kbz bank email ပုံစံမျိုး)
- အသုံးပြုနေကြ (အများအသုံးပြုနေကြ) link များအားအသုံးပြုပြီး click နှိပ်စေခြင်း (www.google.com အစား www.gooogle.com ဟု link တွင်စာလုံးအမှားအသုံးပြုပါသည်)
- စိတ်ပါဝင်စားစေမည့် အကြောင်းအရာကို အသုံးပြုကာ attachment file အား download ယူစေခြင်း (virus ဝင်စေရန်)
- ရင်းနှီးသော လူအမည်အား အသုံးပြုပြီး တစ်ဖက်လူအား ဆွဲဆောင်ခြင်း (luluaung@gmail.com အစား luluaung@outlook.com) ပထမဆုံး Email ပို့တဲ့သူဆီကနေ သူ့ရဲ့ Email server ဆီကိုအရင်သွားပါတယ်.... email server က company , ISP, other location တစ်နေရာရာမှာ ရှိပါတယ် ...ပို့သူ Email Server ကနေ လက်ခံမဲ့သူရဲ့ Email server ဆီရောက်ပါ

မယ်... လက်ခံမဲ့သူက သူ့ Email ကိုဖွင့်ကြည့်ရင် စာဝင်လာတာကိုတွေ့ရမှာဖြစ်ပါတယ် ပုံမှာလဲ ပြထားပါတယ်။ a@gmail.com ကနေ b@yahoo.com ကို mail ပို့မယ်ဆို a@gmail.com ကနေ => gmail.com => yahoo.com ==> b@yahoo.com Forensics သဘောတရားအရကြည့်မယ်ဆိုရင် အပေါ်မှာ ပြထားတဲ့အတိုင်း mail ရှိမဲ့နေရာ ၄ နေရာရှိနေမှာကို တွေ့ရမှာဖြစ်ပါတယ်... အမှုအနေအထားအလိုက် (ISP တွေ mail server တွေနဲ့ချိတ်ဆက်လုပ်ကိုင်ရမှာ ဖြစ်ပါတယ်) Email protocols Simple mail transfer protocol (SMTP) mail ပို့တဲ့နေရာမှာ အသုံးပြုတာဖြစ်ပြီး အလုပ်လုပ်တဲ့ (listening port) နံပါတ်ကတော့ 25 ပါ Domain name Service နဲ့တွဲပြီး အလုပ်လုပ်ပါတယ် Encryption အတွက် SSL or TLS ကိုအသုံးပြုပါတယ်။ A@gmail.com ကနေ B@yahoo.com ကိုမေးလ်ပို့ မယ်ဆိုရင် A ကနေသက်ဆိုင်ရာ SMTP Server ကိုရောက်ပါမယ် SMTP server က ပို့သူနဲ့လက်ခံမဲ့သူကို...ပို့သူ A@gmail.com လက်ခံသူ B@yahoo.com ဆိုပြီး ခွဲထုတ် လိုက်ပါတယ် ပြီးရင် yahoo.com နဲ့ ဆက်သွယ်ပြီး mail ကို exchange လုပ်လိုက်ပါတယ်..လက်ခံသူက POP3 (post office protocol) port no 110 ကိုအသုံးပြုပြီး မေးလ်လက်ခံပါတယ်နောက်ပိုင်း Internet Message Access Protocol (IMAP) port 143 ကိုအသုံးပြုလာပါတယ်။



E-MailHeader

Emailheaderထဲမှာဘာတွေတွေ့နိုင်သလဲဆိုရင် ဘယ်သူကပို့တာလဲ ဘယ်သူ့ဆီကိုလဲ Email Server ဘယ်နေရာတွေဖြတ်လာသလဲ (spam , virus check) ဘယ်အချိန် ဘယ်နေရာနေပို့တယ် (IPaddress) စတဲ့အချက်အလက်တွေပါဝင်ပါတယ် ..Email Header ကိုစစ်ဆေးမယ်ဆိုရင် bottom To Top အောက်ကနေအထက်စစ်ဆေးရပါမယ်..။လူအများဆုံး အသုံးပြုတဲ့ gmail နဲ့ဥပမာ ပြထားပါတယ်။စစ်ဆေးသူက Header ထဲမှာပါတဲ့ အသုံးနှုန်းတွေကို သိရှိထားရမှာဖြစ်ပါတယ်...။ Domain , Ip lookup တွေကိုရှာဖွေတတ်ရပါမယ်။IP address တွေကိုသိရှိနိုင်ပေမဲ့ ip hide လုပ်ထားမယ် Spooof လုပ်ထားမယ်ဆိုရင်တော့ အခက်ခဲ တွေရှိနိုင်ပါတယ်။ အရင်တစ်လောက် Phishing mail တွေ KBZ bank user တွေဆီကို ပို့တဲ့မေးလ်မှာAustralia နိုင်ငံက university တစ်ခုရဲ့ civil law ဌာနမှ mail တစ်ခုကို အသုံးပြုပြီး mail ပို့တာတွေ့လိုက်ရပါတယ်။

```

spf=pass (google.com: domain of edm@emailblast.sg designates 113.197.36.48 as permitted
sender) smtp.mailfrom=edm@emailblast.sg (spam mail check authorized ip or domain)
Received: by server2.emailblast.sg (Postfix, from userid 10001) id 5096D18AE; Wed,
3 Oct 2018 10:33:35 +0800 (+08)
To: koko<koko@gmail.com> (Receiver)
Subject: Join the experts in security related discussions <ady>
X-PHP-Originating-Script: 10001:MailSend.php
From: Myanmar Security Expo <info@myanmarsecurityx.com> (SENDER)
Date: Wed, 03 Oct 2018 02:32:00 +0000 (Arrived Time)
  
```

How To Email Forensics

client ရဲ့ Email Header ကို text သို့မဟုတ် word မှာကူးယူပါ။ Header ထဲမှာပါတဲ့ information တွေကိုသေချာကြည့်ပါ။ မသေသပ်တဲ့ phishing mail ဆိုသိသာပါသည်။ အမှုအနေအထားအလိုက် သက်ဆိုင်ရာ ISP, Mail Server တို့နဲ့ဆက်သွယ်ပါ။

Memory forensics

Ram ဆိုတာ ဘာဖြစ်တယ် ဘာလုပ်တယ်ဆိုတာတော့ အခု post မှာ မပြောတော့ပါဘူး ...

ကွန်ပျူတာ Power Off တာနဲ့ Ram ထဲမှာ သိမ်းဆည်းထားတဲ့ Information တွေပျက်စီးသွားပါတယ် ..

Ram ကနေဘာတွေရနိုင်မလဲ

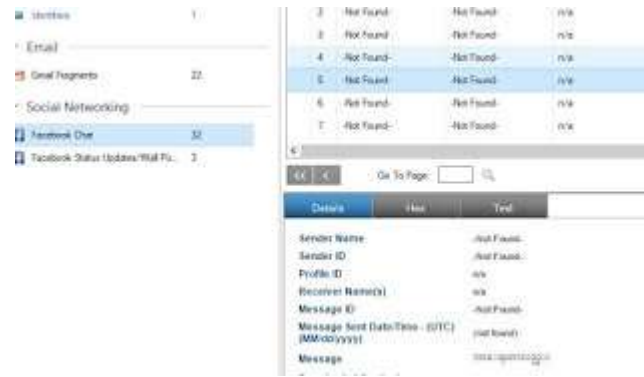
End point Security (antivirus) အချို့က Ram ကိုတိုက်ရိုက်ထိခိုက်စေတဲ့ Virus မျိုးကို မစစ်ဆေးနိုင်ကြပါဘူး ဒါကြောင့် malware Forensics လုပ်တဲ့အချိန်မှာ အသုံးဝင်ပါတယ်

Computer စဖွင့်တဲ့အချိန်မှာ ရိုက်လိုက်တဲ့ username password , Browser History , Internet Connection LAN, Wireless (IP address DNS) , Open Port, Some chat message အစရှိသည်ဖြင့် ရရှိနိုင်ပါသည်။

Memory Forensics ပြုလုပ်ရမည့်အချိန်ကတော့ computer On နေတဲ့အနေ အထားမှာပြုလုပ်ရမှာ ဖြစ်ပါတယ်.. Computer ရဲ့ ram ပမာဏအပေါ်မူတည်ပြီး Memory Dump File Size ရရှိမှာဖြစ်ပါတယ် ။ အခု ကျွန်တော်စက်ဆို 16 GB ရှိတဲ့အတွက် dmp file က 16 GB ရရှိပါတယ်။

အခုအသုံးပြုထားတာတော့ Magnet Memory Forensic နဲ့ Magnet IEF တို့ ဖြစ်ပါတယ်။

ပုံတွေမှာ evidence တွေကတော့ နမူနာပဲပြထားခြင်းဖြစ်ပါသည်။ ကိုယ့် PC ကိုပဲစမ်းထားခြင်းဖြစ်ပါသည်။ Result ထုတ်နေတုန်းရေးထားတာကြောင့်ပါ။



Evidence Device Cloning and Hashing

Investigation လုပ်ရာမှာ မူရင်းသက်သေခံပစ္စည်း (Computer, Laptop, HD, Stick, CD/DVD, Phone) ကို စစ်ဆေးခြင်းမပြုသင့်ပါ။ မူရင်း Device ကို Clone ပွားပြီး စစ်ဆေးရမှာဖြစ်ပါတယ်။ ရလာတဲ့ Clone ကလဲ မူရင်းနဲ့ Hash Value တူရမှာဖြစ်ပါတယ်။ အခု Post မှာတော့ Device တင်မက မူရင်း Device ထဲမှာပါတဲ့ file တွေကိုပါ hash Value ထုတ်ပြထားပါတယ်။

Clone လုပ်တဲ့နေရာမှာ အသုံးပြုထားတာကတော့ Access Data FTK manager ဖြစ်ပါတယ်။ အခြား Clone နဲ့ Hash Value လုပ်နိုင်တဲ့ tools တွေရှိပေမဲ့ နိုင်ငံတကာက Law Enforcement အဖွဲ့တွေအသုံးများတဲ့ Access Data FTK manager ကိုသုံးရခြင်းကတော့ တရားရုံးမှာ သက်သေခံတဲ့အခါ ပိုပြီး Save ဖြစ်အောင်ပါ။

ပုံ (၁) ကတော့ သက်သေခံ မူရင်း Memory Stick Device ရဲ့ Hash value ကို ယူမှာဖြစ်ပါတယ်။ (Stick က ကျွန်တော် Stick ပါ 😊:D) FTK က MD5 and SHA1 ကိုထုတ်ပေးမှာပါ။

ပုံ(၂) မကြာခင် သက်သေခံ မူရင်း Memory Stick Device ရဲ့ Hash value ရလာပါတယ်။ ပုံ (၇) မှာ မူရင်းနဲ့ Clone တို့ရဲ့ Hash Value ကိုပြထားပါတယ်။

ပုံ (၃) သက်သေခံ မူရင်း Memory Stick Device ကို Raw image အနေနဲ့ စစ်ဆေးရန် Clone ယူမှာပါ

ပုံ (၄) မူရင်းဆိုင်ရာ အချက်အလက်ထည့်သွင်းပါမယ်။

ပုံ (၅) Clone ကို သိမ်းထားမယ့်နေရာပါ။ အခြားသူမှားမဖွင့်နိုင်အောင် Password ပါပေးထားပါမယ်။

ပုံ (၆) Password ရိုက်ပါ။ သက်ဆိုင်ရာ CA ထည့်ပါ။ Clone ရိုက်တာကတော့ Device ရဲ့ အရွယ်အစားပေါ်မူတည်ပြီး အချိန်ယူရပါမယ်။

ပုံ (၇) မူရင်း Device နဲ့ Clone Device တို့ရဲ့ Hash value တူရပါမယ်။

ပုံ (၈) မူရင်း Device ထဲမှာပါတဲ့ file တွေကိုပါ hash Value ကိုပါယူထားတာပါ

	A	B	C	D	E	F	G
1	MDS	SHA1	FileNames				
2	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfe95601890afd80709	F:\[root]\[CM]-Memories-of-Murder-(2003)-BRip-				
3	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfe95601890afd80709	F:\[root]\.exe				
4	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfe95601890afd80709	F:\[root]\Removable Drive (16GB).lnk				
5	e3620f6b7ed1a1ce5ab2d56f8a5596fc	4e893a7b5dc280ec3e496d30e192ad184b455ab0	F:\[root]\System Volume Information\IndexerVol.				
6	2637011959e6742db8df829b8e95281d	d38f102461b3b4f3dbf345b9405ed085e4679fe5	F:\[root]\System Volume Information\WPSettings.				
7	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfe95601890afd80709	F:\[root]\Death.Race. 4.Beyond.Anarchy.2018.mp4				
8	4964ef701326baf2759bca6dc6ea3041	8389874b631b17242dd02aed16d320ad2ac578d4	F:\[root]\guardians-of-the-tomb-2018-b.mp4				
9	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfe95601890afd80709	F:\[root]\[CM] The Monkey King 3 (2018) 720p HDT				
10	9eca0c383cb848294f46a6b832459703	0a0b5450dd6610aa3a83a0d6f27be2d83115e76e	F:\[root]\Cloud War 2.mp4				

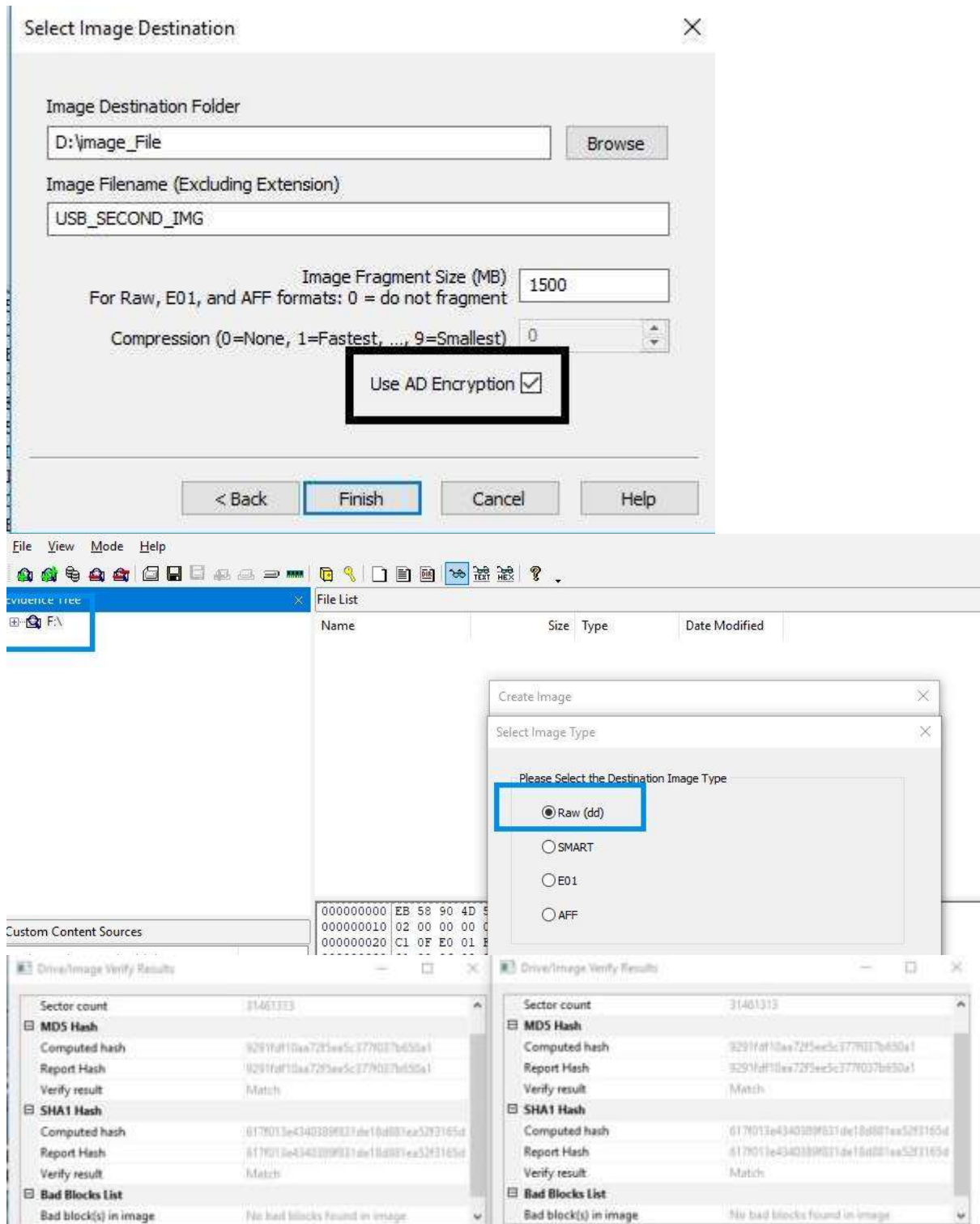
AD Encryption Credentials

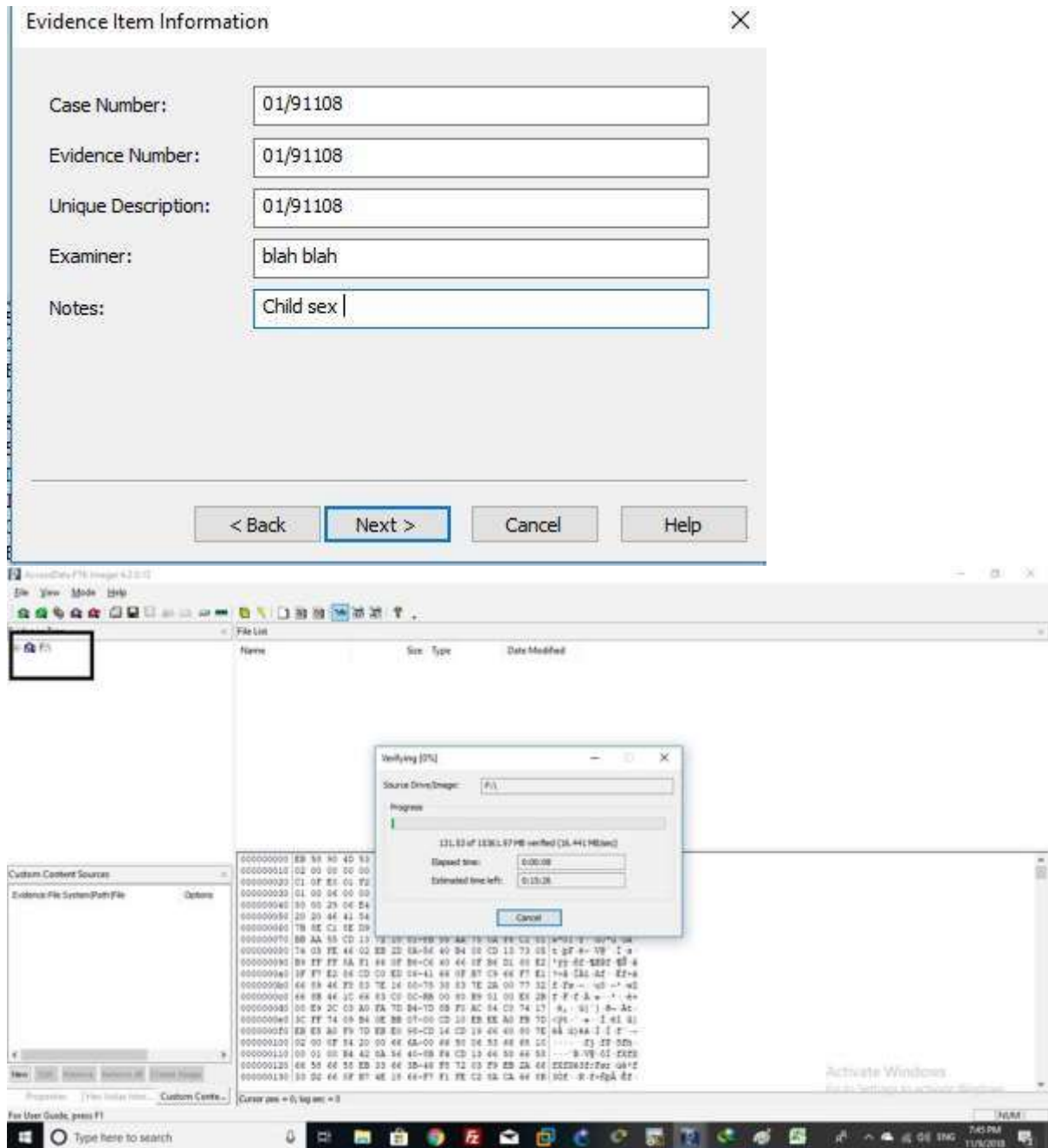
Enter Credentials To Encrypt

☒ Password:

Re-enter: ☐ Show password

☐ Certificate (.pfx, .p12, .pem)





Window Registry Analysis

Window Registry ဟာ ကွန်ပျူတာမှာ အရေးပါတဲ့ အစိတ်အပိုင်း တစ်ခုဖြစ်ပါတယ်။

အသုံးပြုရာမှာ ပိုပြီးတော့ stability နဲ့ Reliability ရှိအောင်ပြုလုပ်ပေးပါတယ်

Window Default Application

Install လုပ်ထားတဲ့ Application

User Information

System Information

Security ပိုင်းဆိုင်ရာ

Network Information

Driver Information စတာတွေပါဝင်ပါတယ် ။

Registry ဟာ Tree ပုံစံနဲ့ဖွဲ့စည်းထားပြီး

Folder နဲ့ File ဖွဲ့စည်းပုံအတိုင်း တည်ဆောက်ထားတာ ဖြစ်ပါတယ်။

Key, Sub key, Name , Data Type , Value တို့ပါဝင်ပါတယ်။

Logical Group ဟာ window ရဲ့ Run Box ကနေ regedit လို့ ရိုက် လိုက်ရင် ပေါ်နေတဲ့ အပိုင်း
၅ ပိုင်းကတော့ Root Folder အပိုင်းဖြစ်ပါ တယ် Key လို့လဲ ခေါ်ပါတယ်

HKEY_CLASSES_ROOT

HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

HKEY_USERS

HKEY_CURRENT_CONFIG

အထက်ပါ ၅ ပိုင်းကိုတော့ တစ်ပိုင်းစီကို Keys လို့သတ်မှတ်ပါတယ်

Key တစ်ခုခြင်းအောက်မှာ သက်ဆိုင်ရာအပိုင်းအလိုက် SubKey တွေရှိပါတယ်။Sub keys
တစ်ခုစီမှာလဲ ဆိုင်ရာဆိုင်ရာ Subkey တွေရှိပါတယ်။

=====

HKEY_CLASSES_ROOT

Software နဲ့ပတ်သတ်တဲ့ Configuration တွေ File System တွေ Shortcut Information
တွေပါဝင်ပါတယ်။အလွယ်ဆုံးပြောရရင် software Shortcut ကိုဖွင့်တာနဲ့ ဘယ် Application
ကိုဖွင့်ရမယ်ဆိုတာကို Window Explorer နဲ့တွဲပြီး အလုပ်လုပ်ပါတယ် ။

HKEY_CURRENT_USER

လက်ရှိဝင်ရောက်တဲ့ User Level နဲ့ပတ်သတ်တဲ့ Software Hardware Configuration တွေကို
သတ်မှတ်ပေးပါတယ်။ Guest Account ဆို Guest Level အလိုက် သတ်မှတ်ပေးပါတယ်။

HKEY_LOCAL_MACHINE

Computer တစ်ခုလုံးရဲ့ Software Hardware အချက်အလက်ကိုဖော်ပြပေးပါတယ်။

HKEY_USERS

လက်ရှိဝင်ရောက်တဲ့ User Level နဲ့ပတ်သတ်တဲ့ Software Hardware Configuration တွေကို သတ်မှတ်ပေးပါတယ်။ သူ့မှာ ဝင်ရောက်အသုံးပြုတဲ့ User အားလုံးရဲ့ အချက်အလက်တွေမှတ်သားထားပါတယ်။

HKEY_CURRENT_CONFIG

လက်ရှိအသုံးပြုနေစဉ်မှာ ဖြစ်နေတဲ့ Hardware အချက်အလက်များကို မှတ်သားထားပါတယ်။

=====

နောက်ဆက်ပြီးဖော်ပြမှာကတော့ Root Folder အောက်မှာ ရှိတဲ့ တစ်ကယ်တန်း အလုပ်လုပ်တဲ့ Physical Group ဖြစ်တဲ့ Registry File Hive File ၅ ခုအကြောင်းပါ။

Software

System

SAM

Security

Default

=====

Software

Default window Setting တွေ Software အချက်အလက်တွေအားလုံးပါဝင်ပါတယ်

System

Computer System တစ်ခုလုံးရဲ့ Hardware အချက်အလက်တွေ အားလုံးပါဝင်ပါတယ်။

SAM

Window ကို login ဝင်ရောက်မဲ့ User account တွေရဲ့ password တွေကို hash File အနေနဲ့သိမ်းဆည်းထားပါတယ်

Security

Security ပိုင်းဆိုင်ရာအချက်အလက်တွေကို သိမ်းဆည်းထားပါတယ်။

Task manager ပိတ်တာ USB သုံးလို့ မရအောင် ပိတ်တာ စသည်ဖြင့်ပါ။ SAM မှာသိမ်းထားတဲ့ အချက်အလက်တွေတော့ မပါဝင်ပါဘူး

Default

User Default Setting ဖြစ်ပါတယ်။ User တစ်ယောက်ဖန်တီးလိုက်တာနဲ့ Window ကိုအသုံးပြုဖို့ Default Configuration ချထားပြီးသားဖြစ်မှာပါ။

=====

Sub key တွေမှာ ရှိတဲ့ Data Type အမျိုးအစားများ

အသုံးအများဆုံးကတော့ .REG_EXPAND_SZ / REG_DWORD / REG_BINARY သုံးခုဖြစ်ပါတယ်။

1.REG_BINARY

Raw Binary Data ဖြစ်ပြီး Hardware အချက်အလက်တွေကို Computer မှ binary data အဖြစ်သိမ်းထားပါတယ်။

Registery editor မှာအကျဉ်းချုံးဖော်ပြနိုင်ရန် Hexa Decimal နဲ့ပြပေးပါတယ်။

2.REG_DWORD

4 byte အရှည်ရှိတဲ့ ကိန်းဂဏန်းများနဲ့သိမ်းဆည်းပြီး Device Driver များ Service နဲ့သက်ဆိုင်သော parameter ကိုဖော်ပြပေးပါတယ်။

Binary သို့မဟုတ် Hexa အနေနဲ့ဖော်ပြပေးပါတယ်။

3.REG_EXPAND_SZ

Program တွေ application တွေကို အဆင်ပြေအောင် သုံးနိုင်ဖို့ အတွက် ပြုလုပ်ပေးတဲ့ variable သည် အခု Data Type အမျိုးအစားမှာ ပါဝင်ပါတယ်။

4.REG_MULTI_SZ

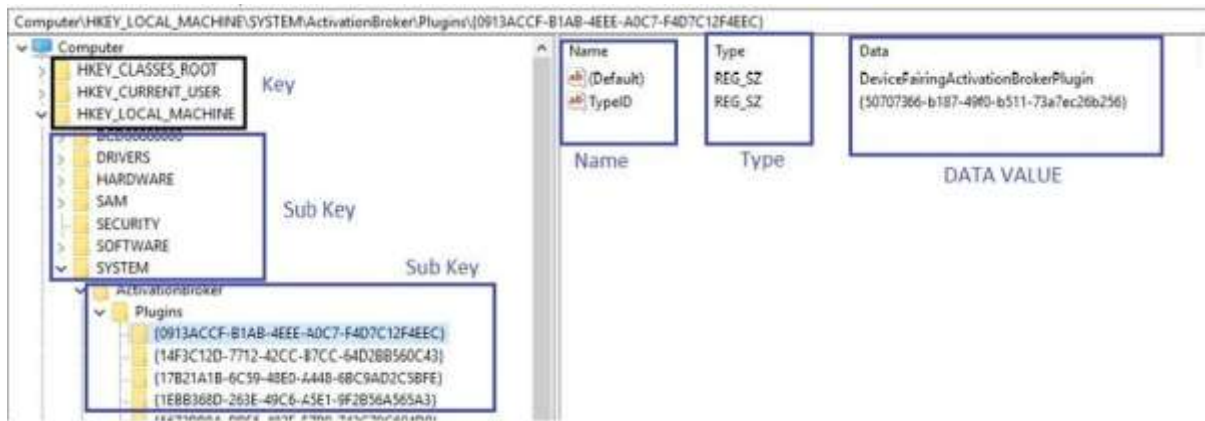
multiple String အမျိုးအစားဖြစ်ပြီး, user များနားလည်နိုင်တဲ့ ပုံစံနဲ့ဖော် ပြထားပါတယ်။

5.REG_SZ

စာသားများပါဝင်ပြီး အလျားသတ်မှတ်ချက်ရှိသော အက္ခရာစဉ် ကိန်းတန်းတစ်ခုကိုဖော်ပြပါတယ်။

6.REG_FULL_RESOURCE_DESCRIPTOR

Hardware အစိတ်အပိုင်း ဒါမှမဟုတ် Dirver တစ်ခုရဲ့ Resource List ကိုသိမ်းဆည်းရန် ဒီဇိုင်းထုတ်ထားသော Nested Array တစ်ခုရှိပါသည်။



Window Registry				
(High Level Key)		(Sub Tree = Root Folder)		
HKEY_CLASSES_ROOT	HKEY_CURRENT_USER	HKEY_LOCAL_MACHINE	HKEY_USERS	HKEY_CURRENT_CONFIG
FILE		(HIVE)		
SAM	Security	Software	System	Default
HKEY_LOCAL_MACHINE	SAM	Security	Software	System
HKEY_CLASSES_ROOT	Software			
HKEY_CURRENT_USER	Software	System		
HKEY_USERS	Default			
HKEY_CURRENT_CONFIG	Software	System		

User တစ်ယောက်ဟာ Window ကိုစတင်အသုံးပြုဆိုတာနဲ့ သူလုပ်ဆောင်သမျှအားလုံးကို Registry ကနေမှတ်တမ်းတင်ထားပါတယ်။

ဥပမာ

Login Time

Account Level

File Open activities

Network Connecting activities

Browser activities

portable device ချိတ်ဆက်မှု စတာတွေကို မှတ်တမ်းတင်ထားပါတယ်။

အချို့သော အချက်အလက်တွေကတော့ Window Shut Down ချတာနဲ့ ပျောက်သွားပါတယ်။

Every things Leave a Trace.

မှတ်သားထားတဲ့နေရာတွေကတော့ part 23 မှာရေးထားတဲ့ key တစ်ခုချင်းစီအောက်မှာရှိနေတဲ့

Sub key တွေ အောက်မှာ သွားသိမ်းဆည်းထားတာပါ။

Registry File location

Windows\System32\Config

ဒါကတော့ registry မှာ တစ်ကယ်အလုပ်လုပ်တဲ့ hive (subkey) တွေရဲ့ Location ပါ။

HKEY_LOCAL_MACHINE \SYSTEM : \system32\config\system

HKEY_LOCAL_MACHINE \SAM : \system32\config\sam

HKEY_LOCAL_MACHINE \SECURITY : \system32\config\security

HKEY_LOCAL_MACHINE \SOFTWARE : \system32\config\software

HKEY_USERS \UserProfile : \winnt\profiles\username

HKEY_USERS.DEFAULT : \system32\config\default

=====

User ဝင်ရောက်တဲ့ အချိန်ကနေ

လုပ်ဆောင်သမျှ ချိတ်ဆက်သမျှကို Registry ကနေ မှတ်တမ်းတင်ထားတယ်ဆိုတာ Part 23 မှာဖော်ပြပြီးပါပြီ။ ... ဘယ်လိုအလုပ်လုပ်လဲဆိုတာနည်းနည်းကြည့်ရအောင်ပါ ...

User တစ်ယောက်က Login ဝင်ဖို့အတွက် Username Password ရိုက်လိုက်တာနဲ့ ရိုက်လိုက်တဲ့

User name ဟာ Registry ထဲက SAM မှာရှိတဲ့ User name နဲ့ တူမတူ တိုက်စစ်ပါတယ်။

Password ကနေ hash generate လုပ်ပြီး SAM ထဲမှာ သိမ်းထားတဲ့ hash

နဲ့တူမတူတိုက်စစ်ပါတယ်။

တိုက်စစ်ပြီးတာနဲ့ တူတယ်ဆိုရင် Window ACL ကနေ အခု login ဝင်တဲ့သူဟာ administrator

လား သာမန် User လား Guest Account လား ဘယ်အဆင့်လဲဆိုတာ ခွဲခြားပါတယ်။

Domain User (AD system) ဆိုရင်တော့ Username အစား Security Identifiers (SIDs)

အနေနဲ့ မှတ်သားထားပါတယ်။ ပြီးရင် ရိုက်လိုက်တဲ့ user name ဟာ

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Profileis

ထဲမှာ ရှိတဲ့ SIDs နဲ့ ကိုက်ညီမှုရှိမရှိ ကြည့်ပါတယ်။ ကျန်တဲ့အဆင့်တွေဖြစ်တဲ့ Password နဲ့ ACL

တိုက်စစ်တဲ့ အပိုင်းကတော့ အတူတူပါပဲ။

User Login pass or fill ဖြစ်တာတွေကို Registry မှာပဲ Event Log အဖြစ်

မှတ်တမ်းတင်ထားပါတယ်။ Security, Software , Hardware warning ပိုင်းကိုလဲ Event log

မှာကြည့်နိုင်ပါတယ် ...

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog

User က Login ဝင်ပြီးတာနဲ့ ဘာ Service တွေ Run မယ် ဘယ် Application တွေက

စမယ်ဆိုတာကို Auto Start လုပ်ဆောင်တဲ့အပိုင်းပါ (Malware အရှိနိုင်ဆုံးအပိုင်းတွေပါ)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001

=====

User က Login ဝင်ရောက်ပြီးတာနဲ့ Wireless or Lan ချိတ်ဆက်မယ် ဆိုရင် ချိတ်ဆက်တဲ့ SSID

Name , DHCP or Static , DNS, စတာတွေကို

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\NetworkCards

အောက်မှ သိမ်းဆည်းထားလိုက်ပါတယ်။ (Volatile information ပါ)

Live System (power on) နေတဲ့ အနေအထားမှာ ဒီအပိုင်းကို စစ်ဆေးရမှာပါ ။

Portable Device တွေ ကွန်ပျူတာမှာ တွဲလိုက်မယ် ဆိုတာနဲ့ ဘယ်နေ့၊ ဘယ်အချိန်မှာ ဘယ်
Device (Serial No) , Device Name ကဆိုတာ မှတ်သားထားပါတယ်။

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\

HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

=====

User ဟာ ကွန်ပျူတာမှာ Firefox Browser ကိုသုံးတာနဲ့ အသုံးပြုတာကို

HKEY_CURRENT_USER\Software\Mozilla\Firefox မှာ မှတ်သားထားလိုက်ပါတယ်။

User တစ်ယောက် လုပ်တောင်မူထဲက အများဆုံးတွေကို

HKEY_CURRENT_USER\software\microsoft\windows\currentversion\Explorer\RunMR
U

မှာ မှတ်သားထားပါတယ်။

User နောက်ဆုံး လုပ်ဆောင်ခဲ့မှုတွေကိုတော့

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Search မှာ
မှတ်သားထားပါတယ်။

User ဟာ Software တစ်ခုကို Install လုပ်လိုက်တာနဲ့

HKEY_CURRENT_USER\Software မှာမှတ်သားထားပါတယ်။

Registry ပိုင်းအနေနဲ့တော့ လုပ်ဆောင်တာတွေ ကျန်ပါသေးတယ် ..

Registry ထဲမှာ မှတ်သားထားတာတွေကို Power on အနေအထားမှာ မှတ်သားတာတွေရှိပြီး
power off အနေအထားတို့မှာဆက်လက်မှတ်သားထားတာတွေလဲရှိပါတယ် ...

Registry အပိုင်းဟာ ရှုပ်ထွေးပြီး စစ်ဆေးမယ်ဆိုရင် အချိန်အတိုင်းအတာ တစ်ခုအထိယူရပါမယ်။ Window Forensics လက်တွေ့လုပ်ဆောင်တဲ့အချိန်မှာ လုပ်ဆောင်ဖို့အခက်အခဲ အနည်းငယ်ရှိပါတယ်။ ဒါကြောင့် Forensics စစ်ဆေးဖို့ tools တွေလိုအပ်လာပါတယ်။

Law Enforcement အဖွဲ့အစည်း ပိုင်းအနေပဲ ဝယ်ယူရနိုင်တဲ့ Tools တွေ Hardware တွေရှိသလို Free ဖြစ်တဲ့ Tools တွေ Hardware တွေလဲရှိပါတယ်။Eg kali, auto spy (current version 4.9) စသည်ဖြင့်ရှိပါတယ်။ More tools Search in Google

အခု Post မှာအဓိက ပြောချင်တာက Forensics Tools တွေက Window Forensic လုပ်ဆောင်တဲ့အခါမှာ Result တွေထွက်လာမယ် ... ထွက်လာတဲ့ Result တွေကို ဉာဏ်ရှိသလို ပိုင်းခြားရှာဖွေရပါမယ်..

ပုံမှာ ပြထားတဲ့ Result တော်တော်များများက window registry ပိုင်းမှာ မှတ်သားထားတာကို Forensics Tools ကနေ စုစည်းပြီး ထုတ်ပေးထားတာပါ။ Window Registry ကိုအဓိက ထားပြီးရေးသားနေတာကြောင့် ကျန်တဲ့ အပိုင်းကို ခန့် ချန်ထားခဲ့ပါမယ်။ (Key point အနေနဲ့ပြောချင်တာက Forensics Tools မှာ ဘာကို စစ်ဆေးမယ် . ဘယ်အပိုင်းကို စစ်ဆေးမယ်, Result တွေထဲက ဘာကိုရှာရမယ်..Result တွေက ဘယ်ကနေ ရရှိလာတယ်ဆိုတာ သိရှိဖို့က Investigator ရဲ့ Knowledge ပါ)

Live system ကို bit by bit (clone) ယူထားတာဖြစ်တဲ့ အတွက် Network information အသေးစိတ်ပါဝင်ပါတယ်။ သိမ်းဆည်းခြင်း၊ image .ယူခြင်း Hashing နဲ့ Write Blocker အပိုင်းကို ကျန်တဲ့ အပိုင်းတွေမှာ ရေးပြီးပါပြီး....

 Classifieds URLs	327
 Cloud Services URLs	702
 Facebook URLs	14963
 Google Analytics First Visit Cookies	77
 Google Analytics Referral Cookies	77
 Google Maps Queries	4
 Google Searches	3082
 Google Translate	11
 Identifiers	36
 Parsed Search Queries	1422
 Social Media URLs	1156
 Torrent URLs	105
Operating System	
File System Information	1
Network Interfaces (Registry)	10
Network Profiles	2
Operating System Information	1
Startup Items	8
Timezone Information	1
USB Devices	32

Investigator Mode - Ca

FileEditToolsGo ToLicensingHelp

Evidence...Go To #:

Web Related

 Chrome Autofill

367

 Chrome Bookmarks

38

 Chrome Cache Records

1210

 Chrome Cookies

3958

 Chrome Current Session

1

 Chrome Current Tabs

9

 Chrome Downloads

181

 Chrome Favicons

5323

 Chrome Keyword Search Terms

1144

 Chrome Last Session

1

 Chrome Last Tabs

29

 Chrome Logins

42

 Chrome Saved Credit Cards

1

 Chrome Shortcuts

495

Hard Disk Forensic . (Part 1) .

Hard Disk တစ်ခုကို forensics မလုပ်ခင် Hard disk ရဲ့ဖွဲ့စည်းပုံကို အရင်ဆုံး သိထားရပါမယ် ...

ပုံမှာ ပါတဲ့ အတိုင်း

Platter ဆိုတာကတော့ Hard disk မှာ Data တွေကို အဓိက သိမ်းဆည်းထားတဲ့နေရာပါ။ Platter ကို ပါးလွှာချောမွေ့တဲ့ aluminum alloy, or glass နဲ့ ပြုလုပ်ထားပြီး meganitic အရည်ကို အပေါ်ကနေ သုတ်ထားပါတယ်။ Platter size ကတော့ 5.25-inch ဒါမှမဟုတ် 3.5-inch ရှိပါတယ်။ platter ရဲ့ အပေါ်ဘက်မှာရော အောက်ဘက်မှာ ပါ data တွေကို သိမ်းထားပါတယ်။ data တွေကို platter ပေါ်မှာ 0 1 အနေနဲ့ သိမ်းထားပါတယ်။ အရင်ကတော့ Hard disk မှာ Platter တွေ 6 ခုလောက်ပါပေမဲ့

နည်းပညာ မြင့်မားလာတာနဲ့ အမျှ platter အရည်အတွက်လည်း နည်းသွားတာကို တွေ့နိုင်မှာ ဖြစ်ပါတယ်။ Platter အရည်အတွက် နည်းတာနဲ့ အမျှ Fault ဖြစ်နိုင်ချေလဲ နည်းသွားပါတယ်။

=====

Spindle ကတော့ platter တွေလည်ပတ်ဖို့ အတွက်လည်ပတ်ပေးရတဲ့ Motor ဖြစ်ပါတယ်။ တစ်မိနစ် လည်ပတ်နှုန်းကတော့ 4,200 RPM ကနေ 15,000 RPM အထိရှိပါတယ်။ လက်တွေ့မှာ အသုံးအများဆုံး Hard disk တွေရဲ့ လည်ပတ်နှုန်းကတော့ 5,400 rpm ကနေ 10,000 RPM အထိရှိပါတယ်။

=====

Head ကတော့ Platter မှာ သိမ်းထားတဲ့ data တွေကို ဖတ်ဖို့ နဲ့ နောက်ထပ် data တွေကို သိမ်းဖို့အတွက်ပါ။ platter တစ်ခုမှာ head ၂ ခုရှိပါဝင်ပါတယ်။ head နဲ့ platter အကွာအဝေးက 0.5 microinches ရှိပါတယ်။ physical damage ဖြစ်တဲ့ hd ကို ပြင်မယ်ဆိုရင် PLATTER SWAP လုပ်တဲ့အခါမှာ HEAD နဲ့ PLATTER ဝေးနေရင် data တွေကို မဖတ်နိုင်ပါဘူး နီးကပ်သွားရင် လည်း platter ပေါ်က data ပျက်စီးနိုင်ပါတယ်။

=====

Actuator

Actuator ဆိုတာ voice coil motor ဖြစ်ပြီး coilထဲကို လျှပ်စစ်စီးဝင်ကာ actuator arm ကိုထိန်းချုပ်ပေးပါတယ်။

=====

Actuator Arm

Actuator Arm ဆိုတာ platter အပြားတွေပေါ်မှာ အလျှားလိုက် ရွေ့နေပြီး data တွေကို သူ့မှာ ပါတဲ့ Head နဲ့ ရေးဖတ်ပေးပါတယ်။

အဲလိုရေးဖတ်တဲ့အခါမှာလဲ အတိအကျဖြစ်အောင် Actuator arm ကို actuator ကပြုလုပ်ပေးပါတယ်.. ။ Arm ရွေ့လျားတဲ့ အခါမှာ အတွင်းကနေ အပြင်ဘက်ကို ရွေ့လျားပါတယ်။

=====

Actuator Axis ဆိုတာ Actuar arm ရဲ့ အစွန်တစ်ခုမှာရှိပြီး axis လည်ပတ်တဲ့ အခါမှာ arm က လိုက်ပါ ရွေ့လျားပါတယ်။

=====

track

track ဆိုတာ ပုံမှန်ပြထားတဲ့ အတိုင်း platter ပေါ်မှာ စက်ဝိုင်းပုံစံအနေနဲ့ ရှိနေတာဖြစ်ပါတယ်။ track အရည်အတွက် များလေလေ သိမ်းဆည်းနိုင်တဲ့ data မမက များလေလေဖြစ်ပါတယ်။ Track Number ဆိုတာကတော့ platter အပြင်ဘက်ကနေ ၀ ဆိုပြီး စတင်ပြီး အပြင်ဘက်သို့ ရေတွက်သွားပါတယ်။ များသော အားဖြင့် track number အစား cylinder အရေအတွက်နဲ့ ဖော်ပြပါတယ်။

=====

Cylinder

platter ပေါ်မှာ data တွေ ရေးဖတ်ဖို့ အတွက်ပြုလုပ်ထားတဲ့ head ဟာ

platterတွေ အပေါ်အောက်မှာ နီးကပ်စွာတည်ရှိနေပြီး တစ်ပြိုင်တည်း တူညီတဲ့ track number အတိုင်းလှုပ်ရှားပါတယ်။ တစ်ကယ်တန်းဆိုရင် cylinder ဆိုတာ platter တွေ ပေါ်က track တွေကို head တိုင်းက access လုပ်နိုင်တဲ့ track အစုအဝေးကို ခေါ်တာဖြစ်ပါတယ်။ နောက်တနည်းပြောရရင် Head တွေတိုင်းက access လုပ်နိုင် တည်ရှိနိုင်တဲ့ platter တွေပေါ်က track အစုအဝေးဖြစ်ပါတယ်။

=====

Sector

Sector ဆိုတာ track ပေါ်မှာ data တွေသိမ်းဖို့အတွက် ဖွဲ့စည်းထားတဲ့အသေးဆုံး physical storage ဖြစ်ပါတယ်။ အရင်ကတော့ sector တစ်ခုမှာ 512 (byte) ရှိပေမဲ့ နောက်ပိုင်း 2010 လောက်ကနေ စပြီး 4,096 bytes (4k) ဖြစ်လာပါတယ်။ ဒါကြောင့် data တွေ ပိုမို သိမ်းနိုင်တဲ့ ပမာဏ များလာတာဖြစ်ပါတယ်။ sector ပါ အပိုင်း ၄ ပိုင်းပါဝင်ပါတယ်

ID information: sector နံပါတ် နဲ့ sector ပေါ်မှာ သိမ်းထားသော data နံပါတ်

Synchronization fields data ကို ဖတ်ဖို့အတွက် ကူညီပေးပါတယ်။

Data: Sector ပေါ်မှာ တစ်ကယ်သိမ်းထားသော data

ECC: data အရေးအဖတ် လုပ်တဲ့အခါမှာ error check , Correction လုပ်တဲ့အပိုင်းပါ

Gaps: data ကိုဖတ်တဲ့အချိန်ရစေဖို့ ပေးတဲ့ နေရာပါ

=====

Cluster

cluster ဆိုတာ hardisk ပေါ်မှာ data သိမ်းဆည်းတဲ့ အငယ်ဆုံးသော logical storage unit တစ်ခုပါ။ data တွေ track ပေါ်က sector ပေါ်မှာ တစ်ဆက်တည်း သိမ်းဆည်းပါတယ်။ အဲလို တစ်ဆက်စပ်တည်းဖြစ်နေတဲ့ sector အစုအဝေးကို cluster လို့ခေါ်ပါတယ်။ HD ကို partation ပိုင်းတဲ့ အပေါ်မူတည်ပြီး cluster size အမျိုးမျိုးရှိနိုင်ပါတယ်။ 4 sector ကို cluster တစ်ခု (သို့) 64,128 ဆိုပြီး ရှိနိုင်ပါတယ်။ cluster size ဆိုရင် $Eg = 4 \times 4k(\text{sector}) = 1600 \text{ byte}$

(slack space ကို သိခြားရှင်းပါမည် forensics လုပ်တဲ့နေရာမှ အရေးကြီးပါသည်)

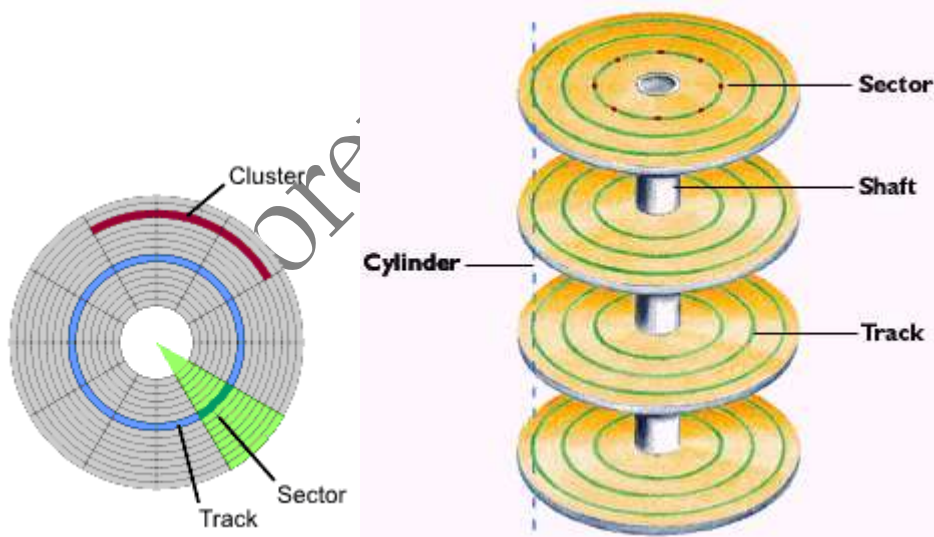
=====

volume

ပိုင်းထားတဲ့ partation logical အပိုင်းဖြစ်ပါတယ်။ Volume တစ်ခုမှာ cluster တွေများစွာပါဝင်နိုင်ပါတယ်။



Tracks, Cylinders, and Sectors



Sector ဆိုတာ track ပေါ်မှာ data တွေသိမ်းဖို့အတွက် ဖွဲ့စည်းထားတဲ့အသေးဆုံး physical storage ဖြစ်ပါတယ်။ အရင်ကတော့ sector တစ်ခုမှာ 512 (byte) ရှိပေမဲ့ နောက်ပိုင်း 2011 လောက်ကနေ စပြီး 4,096 bytes (4k) (Advanced Format) စနစ် ဖြစ်လာပါတယ်။

Bad sector ပျက်စီးနိုင်တာက စက်ရုံကနေထုတ်လိုက်ပြီး သယ်ယူစဉ် ထိမ်းသိမ်းထားစဉ်မှာ ပျက်စီးခြင်း (အဖြစ်နည်းပါသည်)

head နဲ့ platter ကြားမှာ အကြောင်းအမျိုးမျိုးကြောင့် ဖုန်ဝင်သွားတဲ့အခါမှာ read/write head က platter ကို ခြစ်မိပြီး Track ပေါ်က sector များ ပျက်စီးနိုင်ပါတယ်။

hard disk power on နေတဲ့အချိန်မှာ လွတ်ကျတဲ့အခါ / ရုတ်တရက် power Off သွားတဲ့ အခါမှာ sector များ အများဆုံးပျက်စီးနိုင်ပါတယ်။ arm နဲ့ platter တွေ အနေထားမမှန်တဲ့အခါမှာ head က Platter ပေါ်က Track လမ်းကြောင်းပေါ်ရှိ sector တွေကို ခြစ်မိလို့ bad sector ဖြစ်တတ်ပါတယ်။

နောက်တစ်ချက်က sector တစ်ခုခြင်းစီမှာပါတဲ့ ECC ပိုင်း ကနေ file တွေကို error correction မလုပ်နိုင်တဲ့အခါမှာ ဖြစ်တတ်ပါတယ်။ malware ကြောင့်လဲ bad sector ဖြစ်နိုင်ပါတယ်။ အခု အချက် ၂ ချက်ကြောင့် bad sector ဖြစ်တာကတော့ data တွေကို ပြန်လည်ရယူဖို့ အရမ်းမခက်ခဲပါဘူး။

နောက်ပိုင်း hard disk တွေမှာ Hard disk Controller ကနေ bad sector error ဖြစ်နေတယ်လို့ သိရင် bad ဖြစ်နေတဲ့ sector တွေကို မသုံးတော့ပါဘူး မကောင်းတော့တဲ့ sector တွေအစားသုံးနိုင်အောင် Reserved Sectors တွေပါဝင်လာပါတယ်။

=====

Slack Space

Cluster ဆိုတာ hardisk ပေါ်မှာ data သိမ်းဆည်းတဲ့ အငယ်ဆုံးသော logical storage unit တစ်ခုပါ။ data တွေ track ပေါ်က sector ပေါ်မှာ တစ်ဆက်တည်း သိမ်းဆည်းပါတယ်။ အဲလို တစ်ဆက်တည်းဖြစ်နေတဲ့ sector အစုအဝေးကို cluster လို့ခေါ်ပါတယ်။ HD ကို partation ပိုင်းတဲ့ အပေါ်မူတည်ပြီး cluster size အမျိုးမျိုးရှိနိုင်ပါတယ်။ 4 sector ကို cluster တစ်ခု (သို့) 64,128 ဆိုပြီး ရှိနိုင်ပါတယ်။ cluster size ဆိုရင် $Eg = 4 \times 4k(\text{sector}) = 1600 \text{ byte}$

ပုံထဲမှာတော့ sector 3 ခုပေါင်းပြီး Cluster တစ်ခုအဖြစ် ဥပမာ ဖွဲ့စည်းထားပါတယ်။ 10000 bytes ရှိတဲ့ file တစ်ခုကို save မယ်ဆိုရင် sector ၂ ခုနဲ့မလောက်တဲ့ အတွက် နောက် sector ပေါ်မှာပါ ထပ်ယူရပါတယ်။ cluster size က 12000 bytes ရှိတဲ့အတွက် ပိုနေတဲ့ 2000 bytes က slack space ပါ။ နောက်ထပ် file တစ်ခု save မယ်ဆိုရင် ပိုနေတဲ့ 2000 bytes ကနေ စပြီး မသိမ်းတော့ပဲ။ နောက် cluster တစ်ခုကနေ စပြီး သိမ်းမှာ ဖြစ်ပါတယ်။

နောက်ထပ် ဥပမာ အနေနဲ့ 10000 bytes ရှိတဲ့ file ကို cluster 2 ပေါ်ကနေ ဖျက်လိုက်ရင် cluster 2 နေရာက လွတ်သွားမှာဖြစ်ပါတယ်။ နောက်ထပ် 9000 bytes ရှိတဲ့ file တစ်ခုကို ထပ်ပြီး cluster 2 ပေါ်မှာ သိမ်းလိုက်ရင် ပိုနေတဲ့ 3000 bytes က slack space အဖြစ်ကျန် နေမှာ ဖြစ်ပါတယ်။

တော်တော်များများသော paid forensics tools တွေမှာ clone image (or) HD တပ်လိုက်ရင် slack space တွေပါ စစ်ဆေးမလားလို့ choice ရပါတယ်။ အချိန်ပိုမို ကြာပေမဲ့ အချက်အလက် ပိုမိုရနိုင်ပါတယ်။

free ဖြစ်တဲ့ autopsy မှာဆိုရင် slack space ကို သီးခြားခွဲပြီး ကြည့်နိုင်ပါတယ်။

=====

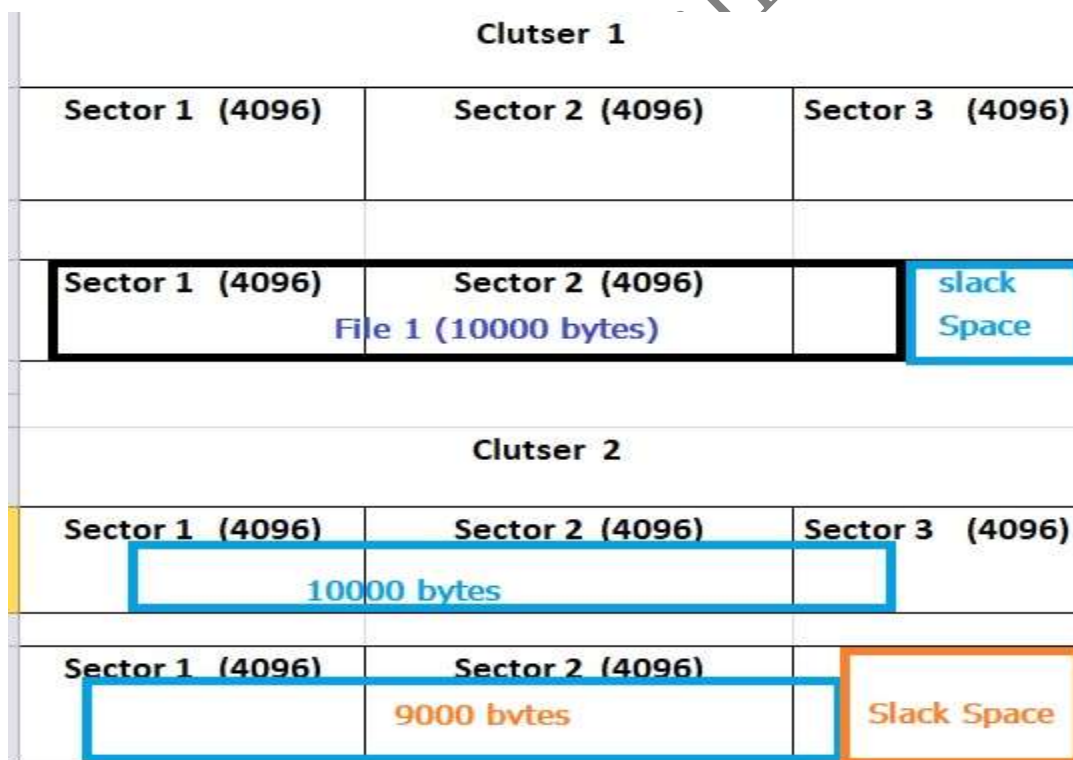
HD firmware

HD firmware ဆိုတာ HD ရဲ့ လုပ်ငန်းစဉ် တွေကို ထိန်းကျောင်းပေးတဲ့ software တစ်ခုဖြစ်ပါတယ်။ spin time , hade read/write , read write speen စတာတွေဖြစ်ပါတယ် ။

HD firmware ကို PCB (Printed Circuit Board) ပေါ်မှာ တစ်ခုတွေ့နိုင်ပါတယ်။ HD power on လိုက်တာနဲ့ Spindle မော်တာကို စလည်ဖို့နဲ့ လည်နေတဲ့ Platter ပေါ်က အချက်အလက်တွေကို ဘယ်နှုန်းနဲ့ ဖတ်ရမည်ဆိုပြီး ညွှန်ကြားချက် ပေးပါတယ်။

နောက်တစ်ခုကတော့ service track (အပြင်ဘက်ဆုံး Track လမ်းကြောင်းပေါ်မှာ ရေးထားတဲ့ firmware ပါ။ သူကနေ microcode တစ်ခုကို ram ပေါ်တင်ပေးပါတယ်။ ပေးလိုက်တဲ့ code ဟာ PCB ကနေ ထုတ်ပေးလိုက်တဲ့ microcode နဲ့ ထပ်တူညီရမှာ ဖြစ်ပါတယ်။

တစ်စိတ်တစ်ပိုင်း ပျက်စီးတဲ့ firmware တွေကို ပြင်ဆင်လို့ရနိုင်ပေမဲ့ လုံးဝပျက်စီးနေတဲ့ firmware ကို ပြင်ဆင်မယ် ဆိုရင် Special Recovery HD set တွေ tools တွေ လိုအပ်မှာ ဖြစ်ပါတယ်။



Boot Loader , Boot Sector , Master Boot Record (MBR) & Window System Boot Process

Boot Loader (Boot manager) ဆိုတာ Program တစ်ခုဖြစ်ပြီး boot လုပ်တဲ့ အချိန်မှာ

Operation system ကို Computer Ram ပေါ်ကို ဆွဲတင်ပါတယ်။ Boot loader မှာ

အဆင့်အမျိုးမျိုးရှိပြီး တစ်ခုနဲ့ တစ်ခု ချိတ်ဆက်အသုံးပြုပါတယ်။ နောက်ဆုံးအဆင့်ကတော့ Operation System တက်လာတဲ့ အဆင့်ဖြစ်ပါတယ်။

Boot Sector ဆိုတာကတော့ Hard Disk ရဲ့ Memory Sector တစ်ခုဖြစ်ပြီး Hard Disk ရဲ့ ပထမဆုံး Track ပထမဆုံး Sector မှာတည်ရှိပါတယ်။

သူ့မှာ bootstrapping system အတွက် code တွေပါရှိပါတယ်။ ဥပမာ အားဖြင့် ပြေရမယ်ဆိုရင် power-on self-test (POST) လုပ်တဲ့ အပိုင်းတွေ ပါဝင်ပါတယ်။ Boot sector မှာ Two Bytes ရှိပါတယ်။ (POST

hardware တွေ ကောင်းမကောင်း စစ်ဆေးသော အပိုင်း)

=====

Boot Sector မှာ အပိုင်း ၂ ပိုင်းပါဝင်ပါတယ်။

Volume Boot Record (VBR)

VBR က HD ရဲ့ ပထမဆုံး Sector မှာ ဒါမှမဟုတ် partition တစ်ခုစီရဲ့ ပထမဆုံး Sector မှာရှိပါတယ်။ Operation System တွေကို loading လုပ်ဖို့အတွက် code တွေပါရှိပါတယ်။

=====

Master Boot Record (MBR) (512 Bytes)

Storage Device ရဲ့ ပထမဆုံး Sector မှာရှိပြီး OS တည်ရှိတဲ့ Partition အပိုင်းကို သိနိုင်စေဖို့ Code တွေပါရှိပါတယ်။ VBR ရှိတဲ့ partition ပိုင်းတွေကိုလဲ သိစေဖို့ code တွေပါရှိပါတယ်။ (multi boot)

MBR ကို Master partition table နဲ့ Master boot code ဆိုပြီး ၂ ပိုင်း တည်ဆောက်ထားပါတယ်။

Master partition table

Storage မှာ ခွဲထားတဲ့ Partition တွေကို သိစေဖို့အတွက် small bit ပမာဏရှိတဲ့ code တွေပါရှိပါတယ်။

Master Boot Code

Boot Process စတင်နိုင်ရန် အတွက် BIOS ကို ဆွဲခေါ်ပေးပါတယ်။ small bit ပမာဏရှိတဲ့ code တွေပါရှိပါတယ်။

=====

HEX Editor တွေနဲ့ MBR , Boot Sector တွေကို ကြည့်နိုင်ပါတယ်။

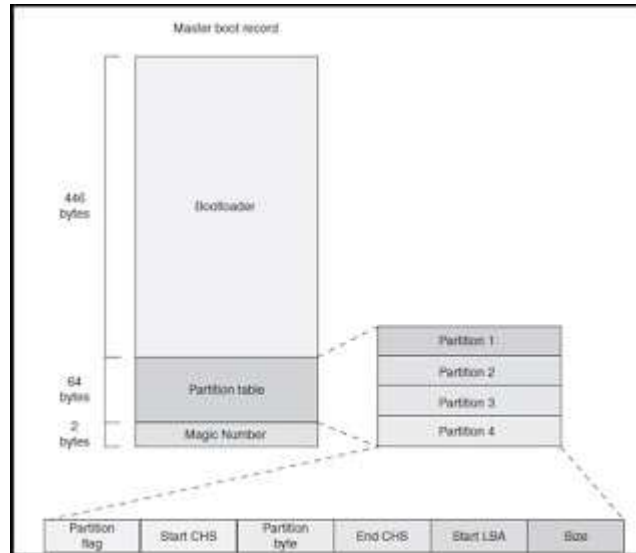
=====

Window System Boot Process

=====

1. Power Supply ကနေ Voltage ရတာနဲ့ CPU ကစတင်အလုပ်လုပ်ပါတယ်။
2. CPU ကနေ ပထမဆုံး BIOS (ROM) ထဲမှာရှိတဲ့ System start up Program တွေကို ကြည့်ပါတယ်။
3. ပထမဆုံး System start up Program အနေနဲ့ the power-on self-test (POST) ကိုလုပ်ဆောင်ပါတယ်။
4. POST က ပထမဆုံး the BIOS chip ကို စစ်ဆေးပြီး CMOS(system date, time, and setup parameters) အပိုင်းကို ထပ်မံစစ်ဆေးပါတယ်။
5. Battery သို့ Power Fail မဖြစ်ဖူးဆိုရင် , POST ကနေ the Computer Hardware Device တွေကို စစ်ဆေးပါတယ်။ DVD, keyboard , Mouse ,extended Harddisk , etc

6. POST စစ်တာ အားလုံးကောင်း မကောင်း : CPU က အတည်ပြုပါတယ်။
 7. The BIOS က CMOS chip ထဲမှာ OS က ဘယ်နေရာမှာ Install ထားတယ် ဆိုတာ ကြည့်ပါတယ်။
 8. ပြီးတာနဲ့ The BIOS ကနေ boot record ကိုကြည့်ပြီး Operation System စတင်ဖို့ OS install လုပ်ထားတဲ့ device နဲ့ OS တက်ဖို့ အတွက် ဆက်စပ်နေတဲ့ Program တွေကို စစ်ဆေးပါတယ်။
 9. OS စတင်ဖို့လုပ်လာတဲ့နဲ့ The BIOS က OS ဆက်တက်ဖို့ လိုအပ်တဲ့ Program တွေကို Memory ပေါ်ကို ဆွဲတင်ပါတယ်။
 10. Memory ပေါ်ကနေ တစ်ဆင့် OS ဆက်လက်တက်ဖို့ လိုအပ်တဲ့ program တွေကို Control ဆက်လုပ်ပါတယ်။
 11. Operation System ကနေ Ram memory အခြေအနေကို ကြည့်ပြီး Operation System ကောင်းမွန်စွာ Run နိုင်ဖို့ လိုအပ်တဲ့ Device Driver တွေကို Run ပါတယ်။
- =====
- OS တွေမှာ ရှိတဲ့ File system တွေ အကြောင်းကတော့ များပြားတဲ့ အတွက် ချန်လှပ်ထားခဲ့ပါတယ်။



Window မှာ file နဲ့ Folder တွေကို ဖျက်လိုက်တဲ့ အခါမှာ ဘာတွေဖြစ်သွားသလဲ ?

ကွန်ပျူတာမှာ file နဲ့ Folder တွေကို ဖျက်လိုက်တဲ့ အခါမှာ ဖိုင် တွေ ဖိဒါတွေရှိတဲ့ Logical Drive နေရာကနေ ကွယ်ပျောက်သွားတာ တွေ့ရပါမယ်။

ဒါပေမဲ့ 0 , 1 အဖြစ်နဲ့ hard disk ရဲ့ Sector တွေပေါ်မှာ cluster အစုအဝေးအနေ နဲ့ ကျန်ရှိနေပါတယ်။

Delete

သာမန် အနေနဲ့ ရိုးရိုး Delete လုပ်လိုက်တဲ့ file , folder တွေက recycle bin ထဲကို ရောက်သွားပါမယ် (file , folder တွေက မြင်နေကြနေရာမှာ မရှိတော့ပါဘူး) (Recycle bin ထဲမှာ မှား ဖျက်မိရင် ပြန်ပြီး Restore လုပ်နိုင်တဲ့ အနေအထားပါ) ။

Recycle Bin ကို clean လုပ်လိုက်တဲ့အခါမှာ Recycle Bin က clean ဖြစ်သွားပါမယ်။ဒါပေမဲ့ data တွေ တစ်ကယ်တန်းရှိနေတဲ့ Cluster ပေါ်မှာတော့ ဆက်လက်ပြီးတည်ရှိနေပါတယ်။

Shift+Delete

Shift+Delete နှိပ်ပြီး ဖျက်တာကတော့ Data တွေက Recycle Bin ထဲကို ရောက်မသွားပဲ
မြင်ကွင်းကနေ ပျောက်သွားမှာပါ။ ဒါပေမဲ့ Hard disk ရဲ့ Cluster ပေါ်မှာ bit တွေ
အဖြစ်ကျန်နေခဲ့ပါတယ်။

=====

Window File System

Microsoft က အရင်တုန်းက သုံးခဲ့တဲ့ File System က fat 16 fat 32 file System
ဖြစ်ပါတယ်။ window 2000 ကနေစပြီး New Technology File System (NTFS)
ကိုစပြီးအသုံးပြုလာပါတယ်။ NTFS မှာ Data တွေက Hard disk ရဲ့ ဘယ် cluster
မှာတည်ရှိနေတယ်ဆိုတာ ပြဖို့ file ၂ ဖိုင်ပါဝင်ပါတယ်။

၁. Master File table (MFT)) Or (Meta File Table)

၂. Cluster Bitmap.

၁. Master File table (MFT)) Or (Meta File Table)

Master File table (MFT)) Or (Meta File Table) ထဲမှာ File အားလုံးရဲ့ File name တွေ၊ file
ရဲ့ Create Date Modified Date တွေ၊ Read Only လား Compressed လား Encrypted
လုပ်ထားတဲ့ file တွေလား ဆိုတဲ့ File တွေရဲ့ အသေးစိတ် အချက်အလက်တွေပါဝင်ပါတယ်။

၂. Cluster Bitmap.

Cluster Bitmap ကတော့ Hard disk မှာရှိတဲ့ Cluster တွေရဲ့ map ကို မှတ်သားထားပါတယ်။
data တွေရဲ့ bit တွေ ဘယ် Cluster မှာရှိနေတယ်။

ဘယ် Cluster ကတော့ အားနေတယ် မသုံးရသေးဘူး စတဲ့ အချက်အလက်တွေ
မှတ်သားထားပါတယ်။

=====

Window ကနေ file တစ်ခုကို delete လုပ်လိုက်တဲ့ အခါမှာတော့

=====

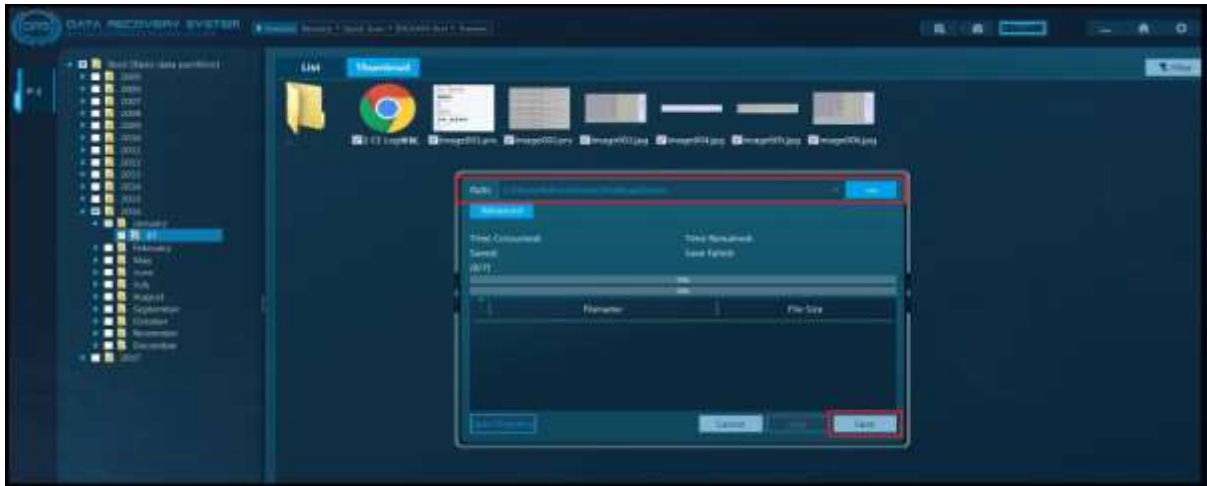
ဖျက်လိုက်တဲ့ file ရဲ့ file name ကို Special Character အနေနဲ့ MFT ထဲမှာပြောင်းလိုက်ပြီး
Processor ကို file ဖျက်လိုက်ပြီး ဖြစ်ကြောင်း အသိပေးလိုက်ပါတယ်။ index field ကို NTFS
မှာပြောင်းလဲပြီး Fat မှာတော့ file name ရဲ့ first letter ကို ပြောင်းလဲပါတယ်။

ဖျက်လိုက်တဲ့အခါမှာ ခုနက file သိမ်းထားတဲ့ Cluster နေရာတွေက လွတ်သွားပါတယ်။
အဲဒါမျိုးမှာ Cluster Bitmap ကနေ cluster ဘယ်လောက်နေရာ လွတ်သွားပြီးဆိုတာ
မှတ်သားထားလိုက်ပါတယ်။ နောက်ထပ် file အသစ်သိမ်းဆည်းနိုင်ရန်အတွက်ပါ။ cluster
ပေါ်မှာ bad sector တွေဖြစ်နေတဲ့အခါ

reversed Sector တွေနဲ့ အစားထိုးတဲ့ လုပ်ငန်းစဉ်ကို ဒီအချိန်မှာ လုပ်သွားပါတယ်။

=====

ဖျက်လိုက်တဲ့ file ကနေယူထားတဲ့ cluster size ကကြီးနေပြီး ၊ နောက် အဲနေရာကို အသစ်ထပ်
save မယ့် file size ရဲ့ Cluster Size ကငယ်နေရင် fragment (Slack Space) တွေဖြစ်နေပြီး
Recovery လုပ်ရတာ လွယ်ကူပါတယ်။



(Redundant Array of Independent Disks) (RAID) (FORENSICS) (Part 1)

=====

RAID စနစ်ကို data များပျက်စီးခြင်းမှကာကွယ်နိုင်ရန်နဲ့ Performance ကောင်းစေဖို့ အတွက် အဓိက ထားပြီးအသုံးပြုကြပါတယ်။ ကိုယ်လုပ်ကိုင်နေတဲ့ အဖွဲ့ အစည်း အသုံးပြုတဲ့ Data တွေပေါ်မူတည်ပြီး Raid Level တွေကို သတ်မှတ် အသုံးပြုနိုင်ပါတယ်။

Raid system မှာ အသုံးပြုတဲ့ နည်းပညာ ၃ ခုရှိရပါတယ်။ အဲဒါတွေကတော့ striping, mirroring, parity, နဲ့ ပေါင်းစပ်အသုံးပြုခြင်းတို့ဖြစ်ပါတယ်။

Striping။

data တွေကို Block Size အနေနဲ့ ပိုင်းလိုက်ပြီး Hard Disk တွေမှာသွားပြီး သိမ်းထားခြင်းဖြစ်ပါတယ်။ Block Size ကတော့ 32KB ကနေ 128KB ,1 MB အသီးသီးရှိပါတယ်။data တွေကို Block အနေနဲ့ ပိုင်းပြီး သိမ်းလိုက်ပြီး array Member တွေဖြစ်တဲ့ Hard disk တစ်ပြိုင်ထဲ သွားပြီး သိမ်းတဲ့အတွက် Read/Write Performance ပိုပြီးကောင်းပါတယ်။ ဒါပေမဲ့ Fault to-le-ran-ce မရပါဘူး။

Mirroring

Data တွေကို Array member ဖြစ်တဲ့ Hard disk တွေပေါ်မှာ သွားပြီး တစ်ပြိုင်တည်း သိမ်းထားခြင်းဖြစ်ပါတယ်။ A ဆိုတဲ့ File တစ်ခုထဲကို Hard disk 1 မှာရော Hard Disk 2 မှာရော သွားပြီး Save ထားခြင်းဖြစ်ပါတယ်။ဒါကြောင့် Fault to-le-ran-ce ရှိပါတယ်။ Read Performance ကောင်းပါတယ်။

Parity

Hard Disk မှာ Data တွေကို သိမ်းထားရင် 0 1 အနေနဲ့ သိမ်းထားပါတယ်။ Parity စနစ်ကတော့ binary number တွေဖြစ်တဲ့ 0 1 တွေအား Xor ကို အသုံးပြုပြီး Parity Data (information) ကနေ Disk တစ်ခု fail ဖြစ်ရင် Fault to-le-ran-ce ရရှိအောင် လုပ်တာပါ။ Xor ကတူရင် 0 မတူရင် 1

(disk 4 မှာ Parity information တွက်ချက်မှု)

Disk 1 = 1 0 1 0

Disk 2 = 1 1 0 0

Disk 3 = 0 0 1 1

Disk 4 = 0 1 0 1 (Parity Information)

when Disk 1 Fail <===== disk 4 က Parity information နဲ့ ပြန် Xor ပါမယ်။

Disk 1 = x x x x

Disk 2 = 1 1 0 0

Disk 3 = 0 0 1 1

Disk 4 = 0 1 0 1 (Parity Information)

Result

Disk 1 = ၁ ၁ ၁ ၁

Disk 2 = 1 1 0 0

Disk 3 = 0 0 1 1

Disk 4 = 0 1 0 1 (Parity Information)

=====

Software Raid = raid 0 (window 7 မှာ ခံနိုင်)

raid 5 , raid 0 = window 8.1 and Window 10

Hardware Raid Controller = SCSI ,SATA, Fiber Channel

=====

RAID 0 (Striping) (Block Size)

=====

- Raid 0 မှာ (Striping) နည်းစနစ်သုံးထားပါတယ်။

- အနည်းဆုံး Same Size Hard Disk 2 လုံး လိုအပ်ပါတယ်။

တစ်ကယ်လို၊ HD တစ်လုံးက 500 GB ဖြစ်ပြီး နောက်တစ်လုံးက

1000 GB ဖြစ်နေရင် အငယ်ဆုံး 500 GB hard disk ကို base

Storage device အဖြစ်ယူပြီး နှစ်ခုပေါင်း 1000GB သာရရှိပါမယ်။

- Read/Write မြန်ဆန်ပါတယ်။

- Fault to-le-ran-ce မရနိုင်ပါ။

RAID 1 (Mirroring)

=====

- Raid 1 မှာ Mirroring စနစ်အသုံးပြုထားပါတယ်။

- အနည်းဆုံး Size တူတဲ့ Hard Disk ၂ လုံးလိုအပ်ပါတယ်။

(Mirroring ဖြစ်လို့ 500 GB 2 လုံးပေါင်းရင် 1000 GB မရပါဘူး 500 GB သာရပါမယ်) ။ 500 တစ်လုံး 750 တစ်လုံးဆိုရင်လဲ 500 GB သာရပါမယ်။

- Read အပိုင်းမှာ မြန်ဆန်ပါတယ်။

- Fault to-le-ran-ce ရှိပါတယ်။

- Fault to-le-ran-ce = (N-1) HD 3 လုံးရှိမယ်ဆိုရင် (3-1) အရ (2)လုံးထိ fail ဖြစ်လို့ရပါသည်)

RAID 5 (Striping with parity)

=====

- Raid 5 မှာ Striping စနစ်နဲ့ Parity စနစ်တို့ တွဲဖက်အသုံးပြုထားပါတယ်။

- အနည်းဆုံး Hard Disk 3 လုံးလိုအပ်ပါတယ်။

- Fault to-le-ran-ce ရှိပါတယ်။

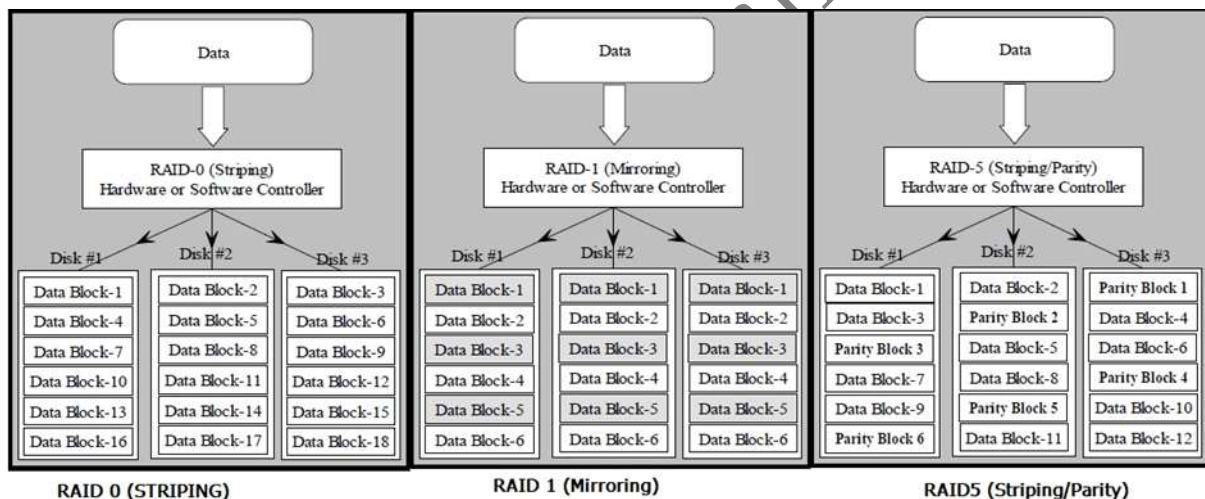
- Read အပိုင်းမှာ မြန်ဆန်ပါတယ်။

- Available Space = (N-1) 500GB hard disk သုံးမယ်ဆိုရင်

(3-1) = 2 အရ 1000 GB သာရပါမယ်။ ကျန် 500 က parity information အတွက်ပါ။

=====

RAID 0 , RAID 1 , RAID 5 ကတော့ လက်ရှိမှာ အသုံးအများဆုံးဖြစ်ပါတယ်။ ကျန်တဲ့ raid တွေကတော့ striping, mirroring, parity, အစရှိတဲ့ စနစ်တွေကို တွဲဖက် အသုံးပြုတာဖြစ်ပါတယ်။ ဒီသဘောတွေနားလည်ရင် အဆင်ပြေပါတယ်။



=====

HOW To Forensics RAID SYSTEM

=====

- how to collect Evidence ကိုအစပိုင်းက ရေးထားပြီးသားအတိုင်းပါ

- မိမိ စစ်ဆေးရမဲ့ ကွန်ပျူတာ, Server က raid level ဘယ်လောက်နဲ့ခွဲထားတယ်ဆိုတာ သိထားရပါမယ်။ Raid 1 ကတော့ ကိစ္စမရှိပါ ဘာလို့လဲဆို raid 1 က Mirroring စနစ်

အသုံးပြုထားတဲ့ အတွက်ကြောင့်ပါ။ raid level ကို auto Detect ဖြစ်တဲ့ forensics နည်းတွေလဲရှိပါတယ်။

- Encase ကိုအသုံးပြုမယ်ဆိုရင် SCSI drive တွေကို auto သိပြီး Volume တစ်ခုထဲအနေနဲ့ မြင်ရပါမယ်။ (Try to ImageHash.....load image and Recover If Need)

(image လုပ်ဖို့ HD storage အခက်ခဲရှိတယ်ဆိုရင် မိမိ Forensics station က SCSI တပ်ဆင်လို့ရပါမယ်။ Or SATA အပိုတွေပါရပါမယ်။

- Example အနေနဲ့ raid 5 ကို ပြထားပါတယ်... ။ ပုံတွေကို ငါးရင်... Sorry ပါခင်ဗျာ...



ကျွန်တော်တို့ Detail ကျကျသွားကြည့်ရအောင်ပါ.. ဒါကြောင့် Crime Case တစ်ခုဖြစ်တဲ့ ရုပ်ရှင်ကား Copy Right ချိုးဖောက်မှုကို Example အနေနဲ့ပြပြီး Forensics လုပ်သွားပါမယ် ။

မှတ်ချက်။ ။ (CHFI နဲ့ CCFP မှာပါတဲ့ example Case များကို ပေါင်းစပ်ပြထားခြင်းဖြစ်ပါသည်။

Case Back Ground

=====

ရုပ်ရှင်ထုတ်လုပ်ရေး Company တစ်ခုမှာ ရုပ်ရှင်ကား တစ်ကားဟာ Editing လုပ်နေတုန်း (RAW file အနေနဲ့) ခိုးယူခြင်းခံရပြီး You tube မှာ တင်လိုက်ပါတယ်။ Company ရဲ့ physical Security ပိုင်း၊ CCTV Camera ပိုင်း ဝန်ထမ်းပိုင်း ကို တစ်ဖွဲ့က စစ်ပါမယ်။ Digital Lab ကိုရောက်လာတာကတော့ Ant PC Ecton SL950X (Work Station) ဖြစ်ပါတယ်။

သူ့ရဲ့ Specific ကတော့ -----

Window 10 64 bit

Processor Brand Intel

Processor Type Core i7 4.2 GHz

RAM Size 16 GB

Hard Drive Size 1 TB + 1 TB (Raid0)

Graphics Coprocessor Nvidia Geforce GTX 1070

Graphics Card Description Nvidia Geforce GTX 1070

=====

Step 1 - Hypothesis အပိုင်းစ စဉ်းစားပါမယ် .. Raid0 ဖြစ်တဲ့အတွက် Striping စနစ်ကို အသုံးပြုထားတယ် , HD က 2 လုံး .. ကူးယူခံရတာက video Raw file (4K) . 100 GB နီးပါရှိတယ်။ အဲအတွက် ကူးယူတဲ့သူက USB ထက် External Hard Disk ကိုအသုံးပြုဖို့များပါမယ်။ အသုံးပြုထားတာက Raid0 စနစ်ဖြစ်တဲ့အပြင် raid0 ပေါ်မှာပဲ window တင်ထားတယ်။ (Network ချိတ်ဆက်ထားရင် တစ်မျိုးထက် စဉ်းစားရပါမယ်)

ဒါဆိုရင် အရှေ့က အပိုင်းတွေမှာ ဖော်ပြခဲ့တဲ့ Window Registry သဘောအရ window ရဲ့ Information တွေက ကျန်ခဲ့ပါမယ်။ user log on time တွေနဲ့ တစ်ခြား အချက်အလက်တွေHard disk သဘောသဘာဝတွေ

Master file table , သဘောတွေ ...

Ok ဒါဆိုရင် အဲဒါချက်အလက်တွေကို တစ်စစီ ဆွဲထုတ်ပါမယ်...

=====

Step 2 - စစ်ဆေးဖို့ Clone လုပ်တဲ့အပိုင်းနဲ့ စစ်ဆေးမယ့်လုပ်ငန်းစဉ် အပိုင်း ဆက်သွားပါမယ်...

Hard disk တွေက physical အရ logical အရ ပျက်စီးမှုရှိမရှိ စစ်ဆေးပါမယ် ... ပျက်စီးရင် raid Recovery process လိုပါမယ်။ ပျက်စီးတဲ့ အပိုင်းက

နောက် ထပ်အပိုင်းနဲ့ လာပါမယ်။ လိုအပ်ရင် Block Level , Parity Level အလိုက် recovery တွေလိုပါမယ်။ အခုအခြေအနေမှာတော့ ပျက်စီးခြင်းမရှိပါဘူး။

raid0 (striping) သုံးထားတဲ့အတွက် hd 2 ခုစလုံးကို clone ယူရမှာဖြစ်ပါတယ်။ ကဲဒါဆိုရင် Encase ရှိတယ်ဆိုရင် တစ်ခြားနည်းနဲ့ Boot တက်ပြီး raid volume ကို Clone ယူရင်ရမယ်။ ဒါမှ မဟုတ် boot တက်ပြီး မယူပဲ HD တစ်ခုစီ ကို Clone ယူ.. ပြီးရင် raid reconstructor နဲ့ Virtual array ဆောက်။

အခြေအနေအရ :D ဒုတိယနည်းကိုပဲ ရွေးလိုက်ပါတယ်။

Forensics Work Station ရဲ့ PCI slot မှာ Raid Recovery / raid connector တပ်ပြီး HD 2 ခုလုံးကို တစ်ပြိုင်တည်း Clone ယူပါမယ်။

Hash ယူပါမယ်။ (Problem အနည်းနည်း တက်တတ်ပါသည် ဒီနေရာမှာ) (တစ်ခုစီ ယူလို့လဲရပါသည်)

ရပြီးတာနဲ့ ... Forensics Kit ဒါမှ မဟုတ် တစ်ခုခုမှာ HD image 2 ခုကို

raid reconstructor အသုံးပြုပြီး Virtual Array တစ်ခု တစ်ဆောက်ပါမယ်။

window Forensics အပိုင်းနဲ့ HD Forensics Concept အပိုင်းကို တွဲလုပ်သင့်ရင်

တွဲလုပ်ရပါမယ်။ ဘယ်နေရာနေစပြီး စစ်ဆေးမလဲ ဆိုတာ စဉ်းစားရပါမယ်။ Window ကနေ ဘာ အချက်အလက်တွေ ရနိုင်လဲဆိုတာ အရင် post တွေမှာ ပြထားပြီးပါပြီ။ :)

ကျန်တဲ့ တစ်ဖွဲ့ စစ်နေစဉ်မှာ ရလာတဲ့ အချက်အလက်နဲ့ digital forensics က ရလာတဲ့ အချက်အလက်ပေါင်းလိုက်ရင် အဆင်ပြေမှာပါ....။

Forensics Methods and Principles (Hypothesis)

Digital Forensics လုပ်ငန်း တစ်ခုလုံးဟာ Scientific Process

လုပ်ငန်းစဉ်တော်တော်များများပါဝင်နေပါတယ်။ ဒါကြောင့် လုပ်ငန်းစဉ်တော်တော်များများဟာ scientific အနေနဲ့ သာလုပ်ကိုင်ရပါတယ်။ Philosophy နဲ့ ပတ်သတ်လို့ 2

ချက်ပါဝင်ပါတယ်။ (Verification နဲ့ Falsifiability) ။ ဒါကြောင့် Digital Forensics Scientific Methods အချို့ကို ဆက်ပြီးတွေးကြည့်ရအောင်ပါ။

ပထမဆုံး Method ကတော့ Hypothesis အပိုင်းဖြစ်ပါတယ်။ hypothesis ဟာ မှန်းဆခြင်း သက်သက်မဟုတ်ပါ။ အမေးရှိရင် အဖြေရှိတယ်ဆိုတဲ့ အတိုင်း မိမိ မှန်းဆချက်ကို forensics လုပ်ငန်းမှာ ရှာဖွေနိုင်ရမယ် ပြီးရင် သက်သေပြနိုင်ရပါမယ်။ ဥပမာ အနေနဲ့ ကြည့်မယ်ဆိုရင် ...

Crime Case Back Ground (NOTE: Base On CHFI&CCFP Note Not Real Wold Case)

=====

Organization တစ်ခုရဲ့ Confidential ဖြစ်တဲ့ PDF တစ်စောင်ပျောက်ဆုံးသွားပါတယ်။ အဲဒီ file ကိုသိမ်းထားတဲ့ ကွန်ပျူတာ ကိုင်တွယ်သူက A ဖြစ်ပါတယ်။ စစ်ဆေးသူက C ဖြစ်ပါတယ်။ (မရွှေမိုး(korea) စာတွေဖတ်တာများလို့ ၊ :D)

ပထမဆုံး စစ်ဆေးသူ C တွေးတာက ကွန်ပျူတာကိုင်တွယ်သူ A ထံကနေ USB Stick 2 ခုလဲ သိမ်းမိတယ်။ A က အဲဒီ File ကို usb နဲ့ကူးတယ်။ ပြီးရင် ဖျက်ထားလိုက်တယ်။ ဒါကြောင့် C က ကွန်ပျူတာကို Forensics Process အတိုင်း စစ်ဆေးပါတယ်။

အခြားအချက်အလက်တွေအပေါ်မူတည်ပြီး သုံးသပ်စစ်ဆေးလိုက်တဲ့အခါ ကွန်ပျူတာကိုင်သူ A က usb ကို တပ်ပြီး file ကိုကူးတာရယ် usb ကို စစ်ဆေးတဲ့အခါမှာလဲ file ကို သိမ်းထားတဲ့ အချက်အလက်တွေကို တွေ့ပါတယ်။ usb ကိုလဲ အကြိမ်ရေများစွာ format ချထားတာကိုလဲ စစ်လို့တွေ့ပါတယ်။ ဒီလောက်နဲ့တင်အချက်လင် Ok နောက်တစ်ဆင့်ကို ဆက်သွားပါမယ်

နောက်တစ်ဆင့်ကတော့ အမူတည်ဆောက်တဲ့အပိုင်းပါ ... သံသယရှိသူ A က ဘယ်အချက်တွေကို မူတည်ပြီး ငြင်းချက်ထုတ်မလဲ တွက်ချက်ပါမယ်..

ပထမငြင်းချက် ...

A က ရုံမှာ အလုပ်မပြီးတဲ့အတွက် အဲဒီ File ကို အိမ်ကိုယူသွားတယ် ..နောက်နေ့ရောက်မှ ပြန်ယူလာတယ် ... အရေးကြီးတဲ့ file ဖြစ်နေလို့ usb ကနေဖျက်လိုက်ပါတယ် လို့ ထွက်ဆိုနိုင်မယ် ... Ok Let it be ...

ဒုတိယငြင်းချက် ...

သူကူးယူတာမဟုတ်ပါဘူး... မသိပါဘူး usb ကလဲ ပျောက်သွားပြီးမှ

စားပွဲပေါ်ပြန်တွေ့တာပါ .. ဆက်သုံးနေတာပါ Ok Let it Be ...

ပထမ ငြင်းချက်ထုတ်နိုင်တဲ့ အတိုင်းကို ပြန်လည်ပြီး သက်သေပြနိုင်အောင်

ထပ်ပြီး စစ်ဆေးရပါမယ်...။ (ဒုတိယ ငြင်းချက်အတွက် လက်ရှိ လုပ်ကိုင်နေတဲ့
အဖွဲ့အစည်းမှာရှိတဲ့ Organization Policy နဲ့ ကိုင်တွယ်ပြီး ထပ်ပြီးသက်သေရှာဖွေပါမယ် ..)
(Note. E- government တွင် Organization Policy သည် အရေးကြီးသော
အချက်အဖြစ်ပါဝင်ပါသည်)

(How To Forensic process အပိုင်းကတော့ အရင် အပိုင်းတွေမှာ ဖော်ပြပြီး ဖြစ်ပါသည်)

ကဲနောက်ဆုံး လုံလောက်တဲ့ သက်သေအချက်အလက် ရပြီဆိုတော့မှ အမှုကို
တည်ဆောက်ပါမယ် (ဒါက Hypothesis အပိုင်းဖြစ်ပါတယ်)

philosophy နဲ့ ပတ်သတ်တဲ့ Verification အပိုင်းဆိုတာကတော့
စမ်းသပ်စစ်ဆေးတဲ့အပိုင်းဖြစ်ပါတယ်။ စစ်ဆေးတဲ့ အချိန်မှာ စစ်ဆေးသူက တွေးရမည့်
အတွေးဖြစ်ပါတယ်။ Falsifiability) အပိုင်းကတော့ ငြင်းချက်ထုတ်နိုင်တဲ့အပေါ်မူတည်ပြီး ထပ်မံ
စစ်ဆေးရမဲ့ အပိုင်း တွေးရမယ့်အပိုင်းပါ။

Locard's principle , inman-Rudin Paradigm အကြောင်းမဖော်ပြခင် ကျန်ခဲ့တဲ့ တစ်ချက်ကို
အရင်ဆုံးဖော်ပြပါမည်။

Peer view

=====

Peer View လို့ခေါ်တဲ့ ပြင်ပကနေ သက်ဆိုင်ရာ Digital Forensics Field ကို ကျွမ်းကျင်တဲ့သူရဲ့
မှတ်ချက် ဒါမှ မဟုတ် ထွက်ဆိုချက်။ တရားရုံးမှာ တစ်ဖက်ရှေ့နေကနေ သက်သေ
အနေနဲ့ သွင်းနိုင်သလို အစိုးရရှေ့နေ ဒါမှ မဟုတ် ကျန်တစ်ဖက်ရှေ့နေကလဲ သွင်းနိုင်ပါသည်။
(နိုင်ငံအလိုက် Cyber Law အပေါ်မူတည်ပါသည်)

=====

Locard's Principle ဆိုတာကတော့ ပြင်သစ်လူမျိုး မူဆင်းဆရာဝန် Dr.Edmond Locard (1877-1907) ဖော်ထုတ်ခဲ့တဲ့ အချက်ပါ။

" မူဆင်းတစ်ခုမှာ ရှာဖွေတတ်ရင် သဲလွန်စကို ရရှိနိုင်ပါသည်ဟူသော အချက်ပါ။ "

ဖော်ထုတ်ချက်ကို Physical Investigation မှာသာ အဓိကထားပြီး

သုံးပေမဲ့ digital ခေတ်ရောက်လာတဲ့ အခါမှာ Theory ကနေ ပြီး ထပ်ဆင့်ချဲ့ယူကြပါတယ်။

Digital Evidence ဆိုတာ ရှာဖွေဖို့ ခက်လဲသလို ပျက်စီးလွယ်ပါသည်။

ဒါကြောင့် ကျန်ခဲ့သော Evidence တစ်ခုထဲကနေ ဖော်ထုတ်နိုင်ဖို့နဲ့ ရရှိတဲ့ Evidence မပျက်စီးအောင် Copy and hashing လုပ်ရမယ်ဆိုတဲ့ အချက် 2 ချက်ဖော်ထုတ်ခဲ့ကြပါသည်။
(Digital Forensics Investigator ရဲ့ EQ IQ Skill အပြင် အခင်းဖြစ်ပွားရာကို အရင်ဆုံးရောက်ရှိ စစ်ဆေးသူရဲ့ Skill ကပါ အရေးကြီးပါသည်) ချွင်းချက်များစွာလဲရှိပါသည်။

inman-Rudin Paradigm

inman-Rudin Paradigm ဆိုတာကတော့ The origin of evidence စာအုပ်ထဲကနေ ကောက်နုတ်ထားတဲ့ အချက်ပါ ...

Transfer အပိုင်းမှာ

(Locard's principle) ကို ရည်ညွှန်းပါသည်။

Identification

Case က ဘာလဲ Evidence ကဘာလဲ

Individualization

ဘယ်လိုသော Evidence အစအန မဆို အရေးကြီးနိုင်သည်။ Case ကို ဘောင်ကျဉ်းအောင် တွေးနိုင်သည်။

Association

သံသယရှိသူနဲ့ ဆက်စပ်ခြင်း

Reconstruction

လိုအပ်ချက်များ လွှဲချောနေမှုများကို ပြန်လည်စဉ်းစားခြင်း

Evidence Transfer & Custody အပိုင်းကို ပြန်လည် စစ်ဆေးခြင်း

ATA Password (SSD and Hard Disk Forensics)

အချို့သော Knowledge ရှိတဲ့ User တွေနဲ့ Organization တွေက BIOS ,UEFI, hard disk password (ATA) တွေကိုထားရုံမက Full Disk Encryption (FED) တွေ Self-Encrypting Drives (SED) နဲ့ပါ တွဲပြီးထားကြပါတယ်။

BIOS password , UEFI pass word တွေကတော့ Forensics process မှာ ခေါင်းသိပ်မခဲရပေမဲ့ Self-Encrypting Drives (SED) တစ်ခုဖြစ်တဲ့

ATA Password မှာ စဉ်းစားရမဲ့ အပိုင်းတွေပါလာပါတယ်။ Googling ရှာ

linux tools / HD tools / boot CD တစ်ခုခုသုံးပြီး Password ကို ဖျက်လို့ရနိုင်ပေမဲ့ data lost ဖို့က 90 ရာနှုန်းလောက်သေချာပါတယ်။

PC Repair ဆိုင်တွေအတွက်ကတော့ အဆင်ပြေချင်ပြေနိုင်ပေမဲ့။ Forensics အပိုင်းကျတော့ detail လဲကျပြီး data တွေကို တတ်နိုင်သမျှဆွဲထုတ်ရမှာ ဖြစ်ပါတယ်။ အဓိကလိုချင်တာက Recovery ပြန်မခေါ်ချင်တဲ့ အချက် ဖြစ်ပါတယ်

ATA password ကို Unlock လုပ်ဖို့အတွက်ဆို.....

User Password အမျိုးအစားကဘာလဲ ?

Master Password အမျိုးအစားကဘာလဲ ?

High နှင့် Maximun Security ကဘာလဲ..... ?

ကိုယ်စစ်ရမဲ့ HD က ဘာအမျိုးအစားလဲ ?

Laptop ကဘာ Model လဲ သူ့ Bios features ?

User password ကိုအခြားသောနည်းများဖြင့် သိရင်အကောင်းဆုံးပါ :)

မသိရင် HD manufacture ကိုသိရင်တော့ Master password ကို ရှာရပါမည်. ။ (Laptop အမျိုးအစားနဲ့ Feature ကိုလဲသတိထားရပါမယ်) (မဟုတ်ရင် Problem အနည်းငယ် တွေ့နိုင်ပါတယ်)

ပုံကတော့ Hardware build နဲ့ ATA password ကိုဖျက်တဲ့ပုံပါ .ဘယ်လိုပင် လုပ်စေကာမူ သဘောတရားကိုတော့ သိထားသင့်ပါသည်။

Platter ဆိုတာ Hard Disk မှာ Data တွေကို အဓိက ထားပြီး သိမ်းတဲ့နေရာ ဘယ်လိုနေရာမှာ ဘယ်လိုသိမ်းတယ်ဆိုတာ ကလေးက အစသိပြီးဖြစ်နေမှာပါ အခု အနေအထား အခုအချိန်ဆိုရင် တစ်ကယ်တော့ Platter မှာခြစ်ရာ ပွန်းရာပါနေတဲ့ အထိ Data ကို အရေးကြီးရင် အရေးကြီးသလို ပြန်ဆယ်လို့ရပါတယ် ... (အခု post အရာတော့ ဒီလောက်အထိပါပဲ)

ဘာလို့လေလုံခန်းလိုသလဲဆိုတာလဲဆိုတာ PLATTER နဲ့ head အကြား

တစ်ကယ်တန်းလိုလားဆိုရင် လိုပါတယ် ရှိရင် ပိုကောင်းပါတယ် ...

ခြားနားချက်လေးတွေပဲရှိတာပါ အဓိက အချက်လေးတွေကိုတော့ Hard disk forensics
အပိုင်းမှာ အချို့ကို ဖော်ပြပြီးပါပြီ ...

=====

- 62

-arm အနေအထားအရ Theory မလွတ်ပဲ စိတ်ရှည်စွာ ဖြုတ်ရပါမယ် (Youtube ကြည့်ပြီး အရေးကြီးလောက်ဘူး ထင်ရပေမဲ့ .. အသေးစိတ် ဂရုစိုက်ရပါမယ် ..)

-Same Doner HD လို့သာ Google Tor youtue တွေမှာဖော်ပြထားပေမဲ့ Theory နဲ့ HD အမျိုးအစားကို လေ့လာထားရင် လက်တွေ့နဲ့ ပေါင်းစပ်ပြီး head နဲ့ Spindle ကိုလဲနိုင် ဖြုတ်နိုင်ပါတယ် ..Platter ကိုလဲနိုင်ပါတယ်

-ပထမအကြိမ်ပျက်နေတာကို ကိုယ့်ကြောင့် ထပ်ပြီး မပျက်ဖို့သာ ဂရုစိုက်ရမှာပါ

=====

- လဲပြီးတဲ့အချိန် spindle လည်သံလဲ ညင်းသာစွာကြားရပြီး .. Head ကလဲ

Platter နဲ့ အမြင်အရ အကြားအရ အဆင်ပြေတယ်.... အလုပ်ရဲ့ 20% ပြီးတဲ့အနေအထားပါ ..ဒီနေရာမှာ အဆင်မပြေရင် 50 ရာနှုန်း Lost ဖြစ်ပါမယ် ..

- rate တွေ time တွေနဲ့ ကျန်အချက်တွေကို Testing လုပ်ရပါအုံးမယ်

- Ok Pass ဖြစ်တယ် ...40% ပြီးပါပြီ

- Recovery ယူမဲ့ အနေအထားရပါပြီး (bad sector , track, cylinder အကြောင်း အသေးစိတ်မဟုတ်တောင် 50 % လောက်နားလည်ထားရပါမယ် ဒီနေရာမှာ)

- ရတဲ့ DATA ပေါ်မူတည်ပြီး ကျန် 60 % က ဘယ်လောက်ရတယ် ဆိုတာပြောလို့ရပါမယ် ...

- ကျန်တဲ့ အပိုင်းတွေဘယ်လိုဆက်လုပ်မယ်ဆိုတာ ဖော်ပြထားပြီးသား ရေးပြီးသားပါ .

Solid-State Drive (SSD) - Forensics

Hard Disk မှာ Spindle မော်တာကြောင့် လည်ပတ်နေတဲ့ Platter တွေ Platter ပေါ်မှာရှိတဲ့ data တွေသိမ်းထားတဲ့ (track,sector,cluster) တွေကို ဖတ်ဖို့ ရွေ့လျားနေတဲ့ Read / Write Head ပါတဲ့ arm တွေပါရှိပါတယ်။ ဒါပေမဲ့ Solid-State Drive (SSD) မှာတော့ လည်ပတ်နေတဲ့ အစိတ်အပိုင်းတွေ မပါဝင်ပါဘူး။ data တွေကို Flash Memory (same as usb stick) ပေါ်မှာ Block အနေနဲ့သာ သိမ်းထားပါတယ်။ လည်ပတ်နေတဲ့ ပစ္စည်းတွေမပါဝင်တဲ့အတွက် vibration ဖြစ်ခြင်းမရှိ၊ အပူထွက်မှုနည်းပါးပြီး HD ထက် အထိအခိုက်ခံတဲ့ အတွက် Solid State Drive လိုခေါ်ဆိုရခြင်းဖြစ်ပါတယ်။

data input-out နှုန်းမြန်ဆန်ခြင်း၊ လျင်ရှားနေတဲ့ အစိတ်အပိုင်းတွေ မပါဝင်တဲ့ အတွက် ထိခိုက်ခံမှုမှာ hard disk ထက်သာလွန်ခြင်း၊ ဆူညံမှုနည်းပါးခြင်း၊ size သေးငယ်ခြင်း၊ Power အစားသက်သာခြင်း၊ data ပမာဏ သိုလှောင်မှုများလာပြီး ဈေးနှုန်းလဲ တစ်ဖြည်းဖြည်းသက်သာလာခြင်းတို့ကြောင့် နောင်တွင်အသုံးပြုမှု ပိုမိုများပြားလာမှာ ဖြစ်ပါတယ်။

SSD မှာ Data တွေကို အဓိက read- write လုပ်တဲ့ Flash Memory ပေါ်မှာပြုလုပ်ခြင်းဖြစ်ပါတယ်။ SSD Flash Memory မှာ သုံးမျိုးရှိပါတယ်။ SSD သက်တမ်းကြာဖို့ TRIM ကိုသုံးနိုင်သလို နောက်ပိုင်း SSD တွေမှာ Wear leveling စနစ်ပါဝင်လာပါတယ်။

SLC (Single-Level Cell) နဲ့ MLC (Multiple-Level Cell) တို့ဖြစ်ပါတယ်။ SLC မှာတော့ Cell တစ်ခုထဲမှာ 1 နဲ့ 0 ထဲကနေ 1 bit ပမာဏကိုသာသိမ်းထားပြီး MCL မှာတော့ Cell တစ်ခုမှာ 2 bit ပမာဏ သိမ်းထားနိုင်ပါတယ်။ Triple Leve Cell မှာတော့ Cell တစ်ခုမှာ 3 bit ပမာဏ သိမ်းထားနိုင်ပါတယ်။ TLC Cell (SSD) တွေက Storage များပေးမဲ့ Performance နှေးပြီး SSD

Life Time လဲနည်းပါးပါတယ်။ အခု user level မှာ အများဆုံးအသုံးပြုနေတာ TLC (SSD) တွေဖြစ်ပါတယ်။

Life time ဆိုတာ SSD မှာ data တွေကို write လုပ်နိုင်တဲ့ အရည်အတွက် ပမာဏ အပေါ်မူတည်ပြီး သတ်မှတ်တဲ့ SSD ရဲ့ သက်တမ်းဖြစ်ပါတယ်။

Controller

Controller Chip ကတော့ SSD ရဲ့ Processor လို့ပြောလို့ရပါတယ်။

အမှန်တစ်ကယ် Data တွေကို သိမ်းထားတဲ့ Flash Memory တွေ နဲ့ SSD ရဲ့ Input-Output Interface ကို ချိတ်ဆက်ပေးပါတယ်။ Error Correction (ECC) အပိုင်းကိုလဲ ဆောင်ရွက်ပေးပါတယ်။ garbage collection, encryption, wear-levelling, , RAISE (Redundant Array of Independent Silicon Elements) အပိုင်းတွေကို ထိန်းညှိပေးပါတယ် ...

Buffer Memory

Buffer Memory Chip ကတော့ သူ့အသုံးပြုထားတဲ့ algorithms နဲ့ Type အပေါ်မူတည်ပြီး data တွေကို မြန်ဆန်စွာရရှိစေဖို့ SSD Input-Output Interface နဲ့ SSD Controller ကြားမှာ ဆောင်ရွက်ပေးပါတယ်။

Input-Output Interface နဲ့ Power Connector ကတော့ SSD အမျိုးအစားနဲ့

အသုံးချတဲ့လုပ်ငန်းနဲ့ Device အပေါ်မူတည်ပြီး ကွဲပြားပါတယ်။ ဥပမာ

SSD SATA ,SSD M2, SSD msata, SSD U2 , SSD Pcie , SSD sas ,

Garbage Collection

SSD မှာ Hard Disk ကဲ့သို့ လှုပ်ရှားနေတဲ့ အစိတ်အပိုင်းတွေမပါဝင်တာကြောင့် data တွေကို read လုပ်ရာမှာရော Write လုပ်ရာမှာရော Hard Disk နဲ့ ကွဲပြားခြားနားမှုရှိပါတယ်။ (HD မှာ data တွေကို read-write ဘယ်လိုလုပ်တယ် Operation ကနေ data တွေကို ဖျက်ရင် ဘယ်လိုဖြစ်တာဆိုတာ အရင် Post များတွင် ဖော်ပြပြီးဖြစ်ပါတယ်)

SSD Flash Memory မှာ Cell တွေစုစည်းပြီး Page , Page တွေစုစည်းပြီး Block ဆိုပြီးရှိပါတယ်။ data တွေကို သိမ်းရင် Page အဆင့်မှာပဲ သိမ်းထားပေမဲ့ erase လုပ်တဲ့အခါဆိုရင် Block အဆင့်ထိပါ ပြုလုပ်ပါတယ်။ (erase နဲ့ delete မတူပါ) page Size က 2KiB, 4KiB, etc ,,,

User က data တွေကို အခြား data သိမ်းထားဆဲဖြစ်တဲ့ Block ပေါ်မှာ သိမ်းချင်တယ်ဆိုရင် ရှိနေတဲ့ Block ထဲက data သိမ်းထားတဲ့ Page တွေကို အခြားလွှတ်နေတဲ့ Block ထဲကူးယူလိုက်ပါတယ်။(ကူးယူပြီးတာနဲ့ flash Controller က ကူးလိုက်တဲ့ data ရှိနေတဲ့ block ရဲ့ logical block address (LBA) ကို အသစ်ထပ်မှတ်လိုက်ပါတယ်။)

data save မှဲ့ page အစုအဝေးဖြစ်တဲ့ Block က Clear ဖြစ်ရင် Erase မလုပ်ပဲ save ပါတယ်။ Clear မဖြစ်ရင် erase လုပ်ပြီးမှ data ကို save ပါတယ်)

program/erase cycles (P/E cycles)

ပြီးရင် အရင် Block ထဲက data တွေကို Erase လုပ်လိုက်ပါတယ်။ဖျက်ပြီးပြီးဆိုတာနဲ့ နောက်ထပ် data သိမ်းနိုင်ကြောင်း flash Controller က Free Block အဖြစ်မှတ်သားထားလိုက်ပါတယ်။ ဒါက Garbage Collection အပိုင်းဖြစ်ပါတယ်။ HD မှာ bad sector ဖြစ်ရင် သုံးဖို့ extra sector တွေပါသလို SSD မှာလဲ extra block တွေပါဝင်ပါတယ်။

Wear leveling

Wear leveling ဆိုတာကတော့ SSD တစ်ခုလုံးမှာ ပါတဲ့ Cell တွေကို အကုန်သုံးနိုင်အောင်ပြုလုပ်ပေးတာဖြစ်ပါတယ်။ program/erase cycles (P/E cycles) ကို ထပ်ကာထပ်ကာ အသုံးမပြုပဲ လွတ်နေတဲ့ Block တွေမှာ data တွေကို write တာဖြစ်ပါတယ်။

Trim (You can use from OS)

Trim ကတော့ Hard Disk Defrag လုပ်သလိုပဲ .. data write ဖို့ block ကိုဖျက်တယ် ...ပြီးရင် ပြန် write တယ်.. data write တဲ့ ပမာဏ (file size)က နည်းလိုက်များလိုက်ဖြစ်လာရင် cell တွေ page တွေ Block တွေက ပျံ့ကျဲလာပါတယ်။ SSD က လေးလာမယ်။ Trim ကို on ထားရင် လွတ်နေတဲ့ block တွေကိုကြည့်ပြီး data ကိုဖျက်ထားတယ် ဒါမှ နောက်ထပ် data save ရင်ပိုမြန်လာမယ်။ Garbage Collection ထပ်ပြီးလုပ်စရာမလိုအောင်ပါ။

(Garbage Collection, Wear leveling , Trim) ကြောင့်ပဲ SSD ကို Forensics လုပ်ရာမှာ challenge တွေရှိလာပါတယ် ...



SSD မှာအများဆုံးသုံးထားတာက NAND flash memory ဖြစ်ပါတယ်။ NOR Flash memory ကိုတော့ အခုအသုံးပြုနေတဲ့ ဖုန်းများမှာ အသုံးပြုထားပါတယ်။ SSD မှာ data တွေကို Write - Delete - Rewrite လုပ်ဖို့အတွက် Garbage Collection , (P/E cycles) , Trim တို့ကို သုံးထားတဲ့အတွက် Data Recovery လုပ်ရာမှာ hard disk နဲ့ သဘောသဘာဝခြင်းမတူသလို လုပ်ဆောင်ရာမှာ ပိုပြီးခက်ခဲပါတယ်။

ဥပမာ HD မှာ file အရေအတွက် 50 ရှိရာမှာ recovery ပြန်လုပ်တဲ့ အချိန် file 40 လောက်ပြန်ရနိုင်ပေမဲ့ SSD မှာတော့ 25-30 files လောက်ပဲရနိုင်ပါတယ်။ Special Forensics tool တွေ Kit တွေနဲ့လုပ်မယ်ဆိုရင်တောင် OS နဲ့ file system အနေ အထားအပေါ်မူတည်ပြီးတော့ မလွယ်ကူနိုင်ပါဘူး :))

ဖြစ်နိုင်ရင် Garbage Collection , (P/E cycles) , Trim အကြောင်းကို နောက်ကျနေအောင် သိထားရင် အကောင်းဆုံးပါ။ အသေးထပ်ထပ်စိတ်ရင်တော့ အကောင်းဆုံးပါ . Process လုပ်ရာမှာ Knowledge ရှိထားရင် ပိုပြီးအဆင်ပြေပါတယ်။ ဖြစ်နိုင်ရင်တော့ EC ပိုင်းကျွမ်းကျင်သူ တွေ နဲ့ အခြားပညာရှင်တွေပါရှိရင်အကောင်းဆုံးပါ

နောက်ထက်သိထားရမှာကတော့ SSD Connector type တွေအကြောင်းဖြစ်ပါတယ်။ SSD ကိုကြည့်ပြီး sata , m2 , u2 , pcie, sas စသည်ဖြင့်သိထားရပါမယ်။ ဒါမှ Work Station ကိုချိတ်ဆက်တဲ့ အခါ ကိုယ့်ဆီမှာ တန်းပြီးတပ်လို့ရရင် တပ် ဒါမှမဟုတ် SSD Connector တွေကိုအသုံးပြုရမှာ ဖြစ်ပါတယ်။

- laptop or PC ကို Forensics Live CD ကပဲ Boot တက်ရပါမယ်။
- SSD ကနေ တိုက်ရိုက် Boot မတက်သင့်ပါ။
- kits or tools or Live CD မှာ auto mount ကို disable ပေးထား ရပါမည်.. Trim ကြောင့်ပါ
- bit-stream copy ကိုသာအသုံးပြုရမှာဖြစ်ပါတယ် ... ။

- SSD connector ကိုချိတ်ဆက်အသုံးပြုရင် သတိထားရပါမယ်။ (kits or tools အလိုက်ကွဲပြားပါတယ်) (same connector ကိုသာ အသုံးပြုပါ (hashing Problem)
- Encryption အပိုင်းမှာတော့ သဘောတရားချင်း ဆင်တူတာရှိသလို ကွဲပြားတာလဲရှိပါတယ်။
- Flash Memory ကိုလဲလှယ်ရာမှာလဲ hard Disk ထက်ပိုမိုလက်ဝင်ပြီး ခက်ခဲပါတယ်။ Memory လဲရာမှာ အမျိုးအစား တူရုံနဲ့တင် မရပါဘူး amount ပါတူမှ ရမှာဖြစ်လို့ပါ။ ကျွမ်းကျင်တဲ့ ပညာရှင်ရော Tool kit တွေပါလိုအပ်မှာပါ
- SSD နဲ့ RAID လုပ်ထားရင်လဲ raid forensics သဘောတရားနဲ့ ပေါင်းစပ်ပြီး လုပ်ရမှာ ဖြစ်ပါတယ်။



Electronic နဲ့ Forensics (Part 39)

Computer or Cyber Forensics ခေါင်းစဉ်တပ်လိုက်တာနဲ့ Aplus Network System web application programing database Crypto mobile ကိုအခြေခံထက်သာအောင် နားလည်ရမယ် တတ်ကျွမ်းရမယ် ဆိုပြီးထင်ကျပါတယ်။ တစ်ယောက်ထဲနဲ့ အကုန်နားလည်ဖို့ဆိုတာ မဖြစ်

နိုင်ပါဘူး.. Forensics လို Detail ကျတဲ့ ဘာသာရပ်ဆို ပိုလိုတောင် မဖြစ်နိုင်ပါ ကျွန်တော်ဆို
Aplus Network, System, Mobile software ပိုင်း ဒီလောက်သာ ရတယ် ဒါတောင် အကုန်
မသိ..မသိခြင်းသည် ရှက်စရာတစ်ခုမဟုတ်ပါ..

လိုက်လို့လဲဆုံးမှာမဟုတ် အသစ်အသစ်တွေက နေ့စဉ်ထွက်နေတာ...အခြားနိုင်ငံတွေမှာတော့
စီးပွားရေးလဲကောင်း အကုန်လုံးကလဲ E goverment ပိုင်းနဲ့သွားနေတာဆိုတော့ Team တွေရော
First Response Team တွေ

ရော သေသေချာချာရှိတယ်..Device လဲမျိုးစုံရှိပါတယ်..

ဒီနေရာမှာ တစ်ခုကွာတာက အာရှနိုင်ငံတော်တော်များများက အနောက်နိုင်ငံတွေက Forensics
Tools Hardware တွေဝယ်သုံးရသည် ...ပြောချင်တာက အနောက်ဘက် နိုင်ငံတွေက ဘာလို့
Forensics

Kits တွေ Tools တွေ ရောင်းနိုင်တာလဲ ... ဝယ်ချင်ရင်တောင် ဒီအတိုင်းသွားဝယ်လို့မရ ... ရောင်
နီနီ ထုတ်နိုင်တယ်

ဆိုတာ တစ်ခုခြင်းစီအလိုက် Detail ဘယ်လိုလုပ်ထားတယ်

ဘယ်လိုတည်ဆောက်ထားတယ် ဆိုတာ သိနေတဲ့အတွက်ပါ ..အချို့ဆို အင်တာနက်မှာပင် နည်း
ပညာကိုရှာမရ ..

သူတို့ဘာလို့လုပ်နိုင်တာလဲ....

.Electronic အကြောင်းကို နောက်ကျနေအောင် သိထား

လို့ ဘယ်နေရာမှာ ဘယ်လိုလုပ်ရင် ဘယ်လိုဖြစ်တယ်

ဆိုတာ သိနေလို့ပါ .အခုဆို အာရှနိုင်ငံကြီးတွေကလည်း

နာမည်ရ Brand တွေထုတ်လာနေပါပြီ..

.ဥပမာ SSD hardware encryption

မှာဆိုရင် user password code က ဘယ်နေရာမှာရှိလဲ

ဘယ်မှာမှ မရှိပါဘူး Password ပေးထားတဲ့ user ရယ်

SSD ထုတ်တဲ့ company ရယ် SSDရဲ့ Firmware (Controller Chip)ထဲမှာသာ ရှိပါတယ်.. User ဆီက Password မသိ မရ Company ကလဲပေးမှာမဟုတ်

ဒါဆိုရင် Controller Chip ထဲမှာပဲရှိမည် ..ကဲ ကိုယ်ဆီမှာ SSD Firmware ကို reverse လုပ်မဲ့သူ ကျွမ်းကျင်တဲ့သူလဲရှိပြီး .. ဒီအတိုင်း ကွန်ပျူတာမှာရေး ဒီအတိုင်းသွားထည့်လို့မရ ... Controller Kit တွေ လိုပြီး ချိတ်ဆက်တဲ့ အပိုင်းတွေလိုပြီ ဖြုတ်ရ ပြန်တပ်ရတဲ့ အပိုင်းတွေလိုပြီ ဒီအကြောင်းကို သိတဲ့ EC သမားရှိမှကိုရတော့မည်.. SSD က Falsh memory ကမတတ်လာဘူး FORENSICS လုပ်ဖို့လဲအရမ်း

လိုနေပြီး ဒါဆိုရင် ဖြုတ်ပြီး တစ်ခြားမှာသွားတတ်ဖို့ပဲ

ရှိသည် စစ်တာကနောက်ထား ဖြုတ်ဖို့ဆင်မလွယ်

Sata SSD က အရမ်းမခက်ခဲ m2 , pcie ဆို တော်တော်

ဒုက္ခရောက်မည်. Flash ကအထိအခိုက်မခံ အမျိုးအစားအလိုက် အထဲမှာ Gate တွေရှုပ်ယှက်ခက် နေသည်..data သိုလှောင်တဲ့ size များလာလေလေ board မှာကို ဟိုဘက် ဒီဘက် flah တွေက ကပ်လျက်ရှိနေသည်

သီးသန့်ဖြုတ်တပ်မဲ့ tools တွေ checking လုပ်ရမည့်

အဆင့်တွေ လိုအပ်လာသည်...သီးသန့် EC သမား

ရယ် SSD ကို Expert ဖြစ်မဲ့သူရယ်က ပထမလိုအပ်လာပါတယ်...သူတို့အဆင်ပြေပြီးဆိုတော့မှ စစ်ဆေးရမဲ့ အပိုင်းက သီးသန့်...HD PCB ဆိုလဲ ဒီအတိုင်းပါပဲ platter Head arm ဖြုတ်တတ်

တာအဆင်ပြေပြီ PCB ပိုင်းပျက်နေရင် EC သမားမရှိရင် ဖုန်သုတ်ပြီး သင်ဒါနဲ့ ဆေးပြီပြန်တပ် ရုံသာရှိမည် :-) Data recovery လုပ်ငန်းတွေက ဒါနဲ့ အဓိက လုပ်နေခြင်းဖြစ်သည်..

Mobile Phone အပိုင်းဆို ပိုလို့တောင် EC ကျွမ်းကျင်တဲ့သူလိုအပ်သည်.. IT ဘက်မှာ application layer ဘက်ကနေပြီး လုပ်တဲ့သူသာ များသည် EC ပိုင်း Softskill ပိုင်းကို ပေါင်းလုပ် နေသူက Product ထုတ်တဲ့သူတွေသာဖြစ်သည်..

လွန်ခဲ့တဲ့ ၆ နှစ်ကျော်က UPS နဲ့ power supply ကို အိမ်တွင်းစီးပွားရေး အနေနဲ့ လုပ်မယ်ဆိုပြီး ကြံကြည့်သေးတယ်...ဘာကြောင့်ပျက်ပျက် လဲပေးမယ်ပေါ့ ကြံတာ :-)

အစိတ်အပိုင်းအလိုက်သေချာတွက်ချက်..လုပ်နေတဲ့နေရာတွေလိုက်ကြည့် ... ကုန်ကြမ်း အဲ မဟုတ်ဘူး ပစ္စည်းကိုအစိတ်အပိုင်းလိုက်ရတယ်..ရာချီသောင်းချီကနေ

သိန်းချီအထိရတယ် အစိတ်အပိုင်းလိုက် Customize တောင် အပ်လို့ရသေးတယ် :-)

.အသေးစိတ်တွက်ကြည့်

တော့ ဘယ်လိုမှမကိုက် မကိုက် :-) ဒါနဲ့ပဲ တရုတ်ကလာတာပဲ ဝယ်သုံးလိုက်တော့တယ် :-)

တစ်ခါကဆိုအလုပ် L3 Switch တစ်ခုက Power ကိုတပ်မလာ... power ပိုင်းကလဲအဆင် ပြေတယ် power ကြိုးလဲတပ်ကြည့်တာကို :-) ဘယ်လိုမှ မရတဲ့အဆုံး ဖုန်ကြောင့်

နေမှာပဲဆိုပြီး ကိုယ့်ဟာကိုယ်တွေ့ ကိုယ့်ဟာကို ဆုံးဖြတ်ပြီး

အဖုံးဖွင့်ဖို့ လုပ်လိုက်တယ် Warranty ကလဲကုန်နေပြီးကို :-) အဖုံးဖြုတ်ပြီးတာနဲ့ ကြည့်လိုက် တော့ အော် L3 Switch ဆိုတာ ဒါကို Circuit Board ရယ် power supply ရယ် Fan ရယ်..EC ပိုင်း ကို ကျွမ်းလို့ပဲ တရုတ်ဆို ပုံတူယူပြီး ဟွားဝေ Switch router တွေထုတ်လာနိုင်တာပဲ...ဒါနဲ့

ထုံးစံအတိုင်း..မြန်မာနည်းမြန်မာဟန်ပဲ ဖုန်သုတ် Mobile ပြင်တဲ့လူတွေသုံးတဲ့ ဆေးဖြန်းပြီးတော့ ပြန် တပ်လိုက်ရတယ်...ကံကောင်းလို့သာပဲ Power ပြန်တက်သွားတယ် :-)

ဘာလို့နည်းပညာနောက်ကျရသလဲ မြန်မာပြည်က

EC ပိုင်းဆို နားလည်သူတွေရှိပေမဲ့ Diode Capacitor မထုတ်နိုင်သေး အချို့အမျိုးအစားတွေဆို နံပတ်မှတ်ပြီး နေရာစုံလိုက်မေး ...ရရင် ကံကောင်းလို့သာပဲ...

အပေါ်အောက်သာ ဆက်ဆံမှုများပြီး အလျားလိုက် ဆက်ဆံမှုပေါင်းစပ်မှုနည်းနေခြင်းနဲ့ မနာလိုစိတ်များနေခြင်းကြောင့်သာဖြစ်သည်..ပြီးရင် ဈေးကွက်နဲ့ စီးပွားရေးမကောင်းတော့ တီထွင် မှုသည်လဲနောက်ကျသွားသည်...

CCTV and DVR Forensics

CCTV and DVR Forensics မှာတော့ investigator က စိတ်ကြိုက်ရွေးချယ်နိုင်တဲ့ အတိုင်းအတာမရှိပါဘူး။ ဆိုလိုချင်တာက CCTV တပ်ဆင်ထားတဲ့သူတွေကလည်း ဘက်ဂျက်အတိုင်းအတာနဲ့ ရွေးချယ်ပြီးတပ်ဆင်တဲ့အပြင် CCTV ကိုတပ်ဆင်ပေးတဲ့သူတွေရဲ့ Setting လုပ်သွားတဲ့အပေါ်လဲမူတည်ပါတယ် ဥပမာ Video File encoding , Hard Disk Wipe Time ။နောက်ပြီး Cable တွေအကွာအဝေး Storage Error Power Source တွေနဲ့လဲ သတ်ဆိုင်ပါသေးတယ်။ ဥပမာ Suspect က ဒီလမ်းအတိုင်းသွားတယ် ... အခုရနေတဲ့ Record က မကြည်လင်ဘူး မပြတ်သားဘူးဆိုရင် ကြည်လင်ပြတ်သားအောင် တစ်ခြားနည်းလမ်းနဲ့ လုပ်ရင်လုပ် မလုပ်ရင် လမ်းတစ်လျှောက်မှ ရှိတဲ့ တစ်ခြား CCTV Record ကိုရယူရုံပဲရှိပါတယ်။ စစ်ဆေးမဲ့သူဟာ CCTV အကြောင်း အနည်းအငယ်တော့ သိထားသင့်ပါတယ်။

လက်တစ်လောမှာ အသုံးများတဲ့ CCTV အမျိုးအစားတွေကတော့

Dome Camera, Bullet Camera, C-mount Camera

Day/Night Camera, PTZ Camera

IP Camera , Portable CCTV Camera တို့ဖြစ်ကြပါတယ်။

Camera နဲ့ DVR ကို ချိတ်ဆက်တဲ့ Cable Type

Coaxial Cable, Siamese Cable (Include Power cable)

Twisted-Pair Cable, Optical Fiber

Video Power Cables, Power Cable

Video နဲ့ Voice Storage လုပ်တဲ့ DVR တွေကတော့

Embedded DVRs

Hybrid DVR

PC-based DVR systems

Self Storage with CCTV Camera

Storage Media

User သုံးနိုင်တဲ့ ငွေပမာဏအပေါ် မူတည်ပြီး အမျိုးမျိုးတပ်ဆင်ကြပါတယ်။ (500 GB, 1 TB, 2 TB)

CCTV အတွက် Enhance ဖြစ်အောင် သုံးတဲ့ Hard Disk အမျိုး

အစားတွဲလဲရှိပါတယ်။

ချိတ်ဆက်တဲ့ Connector Type

Connector Type တွေကတော့ တပ်ဆင်တဲ့ Camera ချိတ်ဆက်တဲ့ Cable အသုံးပြုတဲ့ DVR ပေါ်မူတည်ပြီး အမျိုးမျိုးရှိနိုင်ပါတယ်။

(BNC Male to RCA Female Adaptor , BNC Female to RCA Male Adapter, Female To Female RCA Phono Coupler Adapter, Female To Female RCA Phono Adapter, Co-Axial

RG59 Coax Male BNC Twist On Connector Adapter, Female Jack Connector Adapter ,
etc.....)

CCTV မှရရှိတဲ့ Video နဲ့ Audio Record တွေကို သိမ်းဆည်းတဲ့ File Formant ကတော့
သုံးထားတဲ့ DVR , NVR Type တွေအပေါ်မူတည်ပြီး type မျိုးစုံရှိပါတယ်။ ကွန်ပျူတာပေါ်မှာ
တိုက်ရိုက် ဖွင့်လို့ရတဲ့ type တွေရှိ

သလို တိုက်ရိုက် ဖွင့်လို့မရတဲ့ type တွေလဲရှိပါတယ်။ CCTV Forensics လုပ်တဲ့နေရာမှာ
compression Methods တွေသိထားရင် အထောက်အကူဖြစ်နိုင်ပါတယ်။

နည်းနည်းလောက်ဆက်သွားကြည့်ရအောင် CCTV ကနေကနဦးမှတ်တမ်းတင်လိုက်တဲ့ Video
Raw Data က File Size ကြီးပါတယ် ဒါ့ကြောင့် Cable/Wireless ပေါ်မှာ ပို့လွှတ်ဖို့ရော , Data
သိမ်းထားဖို့အတွက်ရော အခက်အခဲရှိပါတယ်။ ဒီလိုအခက်အခဲမဖြစ်အောင် compression
Methods တွေကို အသုံးပြုပါတယ်။ ယနေ့လက်ရှိအသုံးအများဆုံး Compression Methods
ကတော့ . H.264 ဖြစ်ပါတယ်။ ယခင်ကအသုံးပြုနေတဲ့ MPEG-4 , MJPEG တွေထက် Video
Compression ပိုင်းမှာ ပိုကောင်းပါတယ်။ Storage ပမာဏ အနည်းဆုံးနဲ့ Video Quality
အကောင်းဆုံးဖြစ်အောင် Compression လုပ်ပေးပါတယ်။ Transmit ပိုင်းမှာလဲ bandwidth (bit
rate) အနည်းဆုံးနဲ့ transmit လုပ်ပေးပါတယ်။ အခြား Compression Type တွေမှာတော့
Frame rate (frames per second-Fps) တွေ ဒါမှမဟုတ် Resolution တွေကို ပြောင်းလဲပြီး
Video အချိန်ချိန်ကြာကြာ သိမ်းထားနိုင်အောင် bandwidth
အစားသက်သာအောင်လုပ်ထားပါတယ်။

=====

H.264 ဘယ်လိုအလုပ်လုပ်သလဲ

Camera ကနေမှတ်တမ်းတင်လိုက်ပြီးတာနဲ့ H.264 Encoder ဆီကို Compressed လုပ်ဖို့ data
Frame တွေပို့လွှတ်လိုက်ပါတယ်။

H.264 Encoder မှာ Methods နှစ်မျိုးနဲ့ Compressed လုပ်ပါတယ်

I-frame နဲ့ P-frame တို့ ဖြစ်ပါတယ်။

Camera ကနေ စစ်ရိုက်ချင်း Compressed မလုပ်သေးပဲ I-Frame နဲ့ စတင်ရိုက်ပါတယ်။

Play Back Forward Backward Seeking time စတာတွေကို ပြန်ကြည့်နိုင်အောင်ပါ။

P-Frame ကတော့ ပထမရိုက်ထားတဲ့ Frame နဲ့ ဒုတိယ ရိုက်ထား

တဲ့ Frame ကိုပြန်ကြည့်ပြီး Motion ဒါမှ မဟုတ် Back Ground အနေ

အထားမပြောင်းလဲရင် ထပ်ပြီးတော့ Save မလုပ်တော့ဘူး။ Motion ဒါမှ မဟုတ် Back Ground ပြောင်းမှသာ ထပ်ပြီး save ပါတယ်။ ဒါကြောင့် Storage အစားသက်သာသွားတာပါ။

အသုံးအများဆုံး File type တွေကတော့

H.264 , H.265 , MPEG-4 Part 10,

MPEG-4 part 2, JPEG, MPEG-2

.dav, .asf files, .avi

=====

Part 41 42 မှာ How to CCTV Forensics ရယ် သတိထားရမဲ့ အချက်တွေရယ် Principle တွေအကြောင်းဆက်ပါမယ်။ Thanks

First Responder အပိုင်း Chain of Custody အပိုင်းတွေက ဖော်ပြပြီးဖြစ်လို့

သီးသန့်မဖော်ပြတော့ပါဘူး။ Lab ကိုရောက်လာတဲ့ အချိန်မှာ CCTV Record ဟာ DVR

သို့မဟုတ် DVD ,Stick အစရှိသည်ဖြင့် ပုံစံမျိုးစုံနဲ့ ရောက်ရှိလာနိုင်ပါတယ်။

အကောင်းဆုံးကတော့ DVR ဒါမှမဟုတ် မူရင်း Storage media ကတော့ အကောင်းဆုံးပါ။

တစ်ဆင့်ခံအနေအထားနဲ့ ရောက်ရှိလာရင် Resolution အနေအထား Evidence
ကောက်ချက်ဆွဲမှုတွေမှာ ကန့်သတ်ချက်တွေရှိလာနိုင်ပါတယ်။

DVR, NVR အတိုင်းရောက်ရှိလာတာလား

(DVR အခြေအနေ) (အမျိုးအစား)

Storage ပဲရောက်ရှိလာတာလား (Storage Size)

Storage အတိုင်းဆိုရင် DVR ရဲ့ setting ကဘယ်လိုမျိုးလဲ

(DVR ဒါမှမဟုတ် Storage media fill ဖြစ်ရတဲ့ အကြောင်းအရင်းတွေလဲသိထားရပါမယ်)

အစရှိသည်ဖြင့် စစ်ဆေးရပါမယ် ... ကျန်စစ်ဆေးရမဲ့ အပိုင်းတွေကတော့

စာရည်နေမှာမို့ မရေးတော့ပါဘူး။ အချို့သော လူတွေကတော့ record မပေးချင်တဲ့ အတွက်ရော
မပေါ်ချင်တာရောနဲ့ အမျိုးမျိုး လိမ်လည်နိုင်ပါတယ်။ မည်သို့ပင်ဆိုစေ နည်းပညာအရ
စစ်ဆေးနိုင်သော နည်းလမ်း

များစွာရှိပါတယ်။ :)

Storage အပိုင်း Fill ဆိုရင်တော့ မူခင်းအလိုက် Concept နဲ့ အတူ Hard Disk Recovery

Concept နဲ့ ဆက်စပ်လုပ်ဆောင်ရပါမယ်။ Recovery ပိုင်းမှာ

နည်းနည်းလောက်ကွဲပြားတာရှိပါတယ်။

စစ်ဆေးတဲ့ Theory တွေထဲကမှ အရေးကြီးတဲ့ အချက်တွေကတော့

Image enhancing လုပ်တဲ့အပိုင်း (example Image Transcoding)

Tracking The Target (more Source Require...)

Comparing (image database Require)

Demonstrative Comparison

Height Calculating

etc အစရှိသည်ဖြင့်ရှိပါတယ်။

CCTV ,DVR Forensics သဘောတရား အပြင် အခြားလိုအပ်တဲ့အချက်တွေကတော့ HR

အင်အားရယ် စိတ်ရှည်မှုရယ်ပါ။ IQ EQ AQ အကုန်လုံးကို အသုံးပြုရမှာဖြစ်ပါတယ်။

ဆက်စပ်အသုံးပြုရမဲ့ Hard ware တွေရဲ့ စွမ်းဆောင်ရည်ကလဲ အရေးကြီးပါတယ်။

စစ်ဆေးပုံအချို့ကို example case အနေနဲ့ကြည့်မယ်ဆိုရင် ပထမပုံက

bamakhit ကနေ မကြာသေးခင်ကမှ တင်ထားတဲ့ မွန်ပြည်နယ် ကျိုက်ထိုမြို့၊ သေနတ်နဲ့ အနကြမ်းစီးတဲ့ CCTV ကို ခွဲခြမ်းစိတ်ဖြာထားပုံပါ။(Download ယူပြီး စမ်းထားတာပါ :)

Video File က Low Resolution အနေအထားဖြစ်နေပါတယ်။ Resolution ကို

အနည်းငယ်ပြောင်းကြည့်ပါတယ်။ မူရင်းမကောင်းတဲ့အတွက်ရော Resolution

ပိုင်းကျွမ်းကျင်သူလိုအပ်တာရော Hardware အနေအထားအရရော

အနည်းငယ်သာပြောင်းလဲပါတယ်။

ပြီးရင် အနေအထားအရ 1 မိနစ်စာ Video file ကို လှုပ်ရှားမှုအလိုက် ထပ်ပြီးခွဲခြားလိုက်ပါတယ်။

ကျွန်တော် နမူနာ ခွဲခြားထားတာက အနေအထားပေါင်း 410 ရရှိပါတယ်။ ခွဲဖြာပုံအလိုက်

ပြောင်းလဲနိုင်ပါတယ်။ ဘာလို့ခွဲခြားရလဲဆိုရင် အပိုင်းတွေများစွာထဲကနေမှ ဆက်စပ်သုံးသပ်ပြီး

တရားရုံးမှာ သက်သေခိုင်လုံအောင် တင်ပြနိုင်အောင်ပါ။

ဒုတိယပုံ တတိယပုံ ကတော့ cambodia က Case ပါ Resolution အနည်းငယ်ကောင်းပါတယ်။
ဖုန်းလုတဲ့ CCTV မှတ် တမ်းပါ။ အသေးစိတ် လှုပ်ရှားမှုအလိုက် ခွဲခြမ်းပြီး ယူထားပါတယ်။ Motion
များစွာပါတဲ့အတွက် 600 ကျော်လောက်ထိရနိုင်ပါတယ်။ နည်းပညာအပြည့်အစုံရယ် စစ်ဆေးပုံ
တွေးဆပုံ အကြောင်းအရာ အပြည့်အစုံ ကိုတော့ ငွေမယ့် အခြားသော အဖွဲ့အစည်းတွေရှိလို့
အပြည့်အစုံမရေးခဲ့နိုင်တာ Sorry ပါ။ ဒီလောက်ဆို ဆက်စပ်ပြီးလေ့လာလို့ရပါပြီ။ Print Screen
ကြောင့် ပုံအရည်အသွေးသိပ်မကောင်းပါ။



Raspberry Pi Forensics

Raspberry Pi ဆိုတာ ဘယ်လိုမျိုးလဲ ဘာလုပ်လို့ရလဲ ဆိုတာ IT EC ပိုင်းကလူတွေ
သိပြီးသားပါ။ ARM-Based RISC OS Plan 9 FreeBSD Chromium OS Windows 10 IoT

AmigaOS IchigoJam BASIC Kali * စတဲ့ OS တွေ တင်နိုင်ပါတယ်။ အခုဆိုရင် Raspberry Pi 3 Model B အထိရောက်လာပါပြီ။ အရင် Model တွေမှာ မပါတဲ့ WiFi Blue tooth စနစ်တွေပါဝင်လာပါတယ်။ ပိုပြီး portable

ဖြစ်လာပါတယ်။အဲ့တော့ Pentest အတွက်လဲ အသုံး

ချနိုင်သလို Remote အနေအထားနဲ့ရော , WiFi Base အနေအထားနဲ့လဲ အသုံးချလာနိုင်ပါတယ်။ အခုအချိန်မှာ ဖြစ်မလာပေမဲ့ နောင်တစ်ချိန်မှာ ဖြစ်လာနိုင်ချေတွေ အတွက်ပါ။

Raspberry Pi မှာ OS loading အတွက်ရော Storage အတွက်ရော USB, SD card Class 10 ကိုတော်တော်များများအသုံးပြုကြပါတယ်။

အချို့ သော Raspberry Pi တွေမှာတော့ memory အတွက် Chip ကိုအသုံးပြုပါတယ်။ OS တော်တော်များများကတော့ linux Base ဖြစ်တဲ့ အတွက် File System ကတော့ Ext4 ဖြစ်ပါတယ်။

How To Forensics

ဘယ်အချိန် ဘယ်နေရာမှာ ဘယ်လိုအနေအထားနဲ့ အသုံးချတာလဲ

(When where and How)

ဘာတွေနဲ့ချိတ်ဆက်ထားလဲ

(How to Connect With)

ချိတ်ဆက်ထားတဲ့အတွက် ဖြစ်မလဲ ... ?

(What Happen ?)

Imaging and hasing ပိုင်းမှာ သတိထားရပါမယ်.

Connector ကောင်းရပါမယ်

SD, USB , linux Forensics အပိုင်းနဲ့ ဆက်စပ်ရပါမယ်



Vmware Forensics

လက်ရှိသုံးနေတဲ့ Operation System ပေါ်မှာပဲ အခြားသော Operation System ကို အကြောင်းရင်းတစ်ခုခုကြောင့်သုံးခြင်တယ်ဆိုရင် Virtual System တစ်ခုကို အသုံးပြုကြပါတယ်။ အသုံးများတဲ့ Virtual System တွေကတော့

Virtual Box

VMware

Window Virtual PC

Hyper -V

Oracle VM

Parallels

Docker တို့ဖြစ်ပါတယ်။

ဒီထဲကမှာမှ Vmware Forensic အကြောင်းကို ရေးသားသွားပါမယ်။ ဘာလို့လဲဆိုရင် VMware forensics အကြောင်းသိရင် Esxi, Vspher ,Vcenter Forensics အကြောင်းကိုပါ ဆက်စပ်လေ့လာနိုင်အောင်လို့ပါ။

Esxi, Vspher ,Vcenter Forensics အကြောင်းကတော့ တော်တော်လေး ရေးယူရမဲ့ အပြင် လက်တွေ့ပြနိုင်မှ ပိုအဆင်ပြေမှာမို့လို့ပါ။

Vmware မှာပါတဲ့ file system တွေကတော့

vmem - Virtual machine memory file

vmdk - Virtual machine storage disk file

vmss - Virtual machine information file

log - Virtual machine log file

nvrAm - Keeps VM's BIOS information

vmsn - Virtual machine snapshot file

vmxf - Additional configuration file.

.Vmdk

.Vmdk ကတော့ VMware Forensics မှာ အရေးကြီးတဲ့ အပိုင်းမှာ ပါဝင်ပါတယ်။ VMware မှာပါဝင်တဲ့ အချက်အလက်တွေ အကုန်ပါဝင်ပါတယ်။ VMware Hard disk နဲ့လဲ ချိတ်ဆက်ပေးပါတယ်။

.vmem

.vmem ကတော့ ကွန်ပျူတာမှာ အသုံးပြုနေတဲ့ Ram တွေလိုပဲ

VMware ရဲ့ memory ပါ။ ဒါဆိုရင် အရင်ကရေးခဲ့တဲ့ Memory Forensics

အတိုင်း Forensics လုပ်လို့ရနိုင်ပါတယ်။ vmem ကနေဘာတွေရနိုင်မလဲ

User account, Password, Chat history, Web browsing history စတာတွေရရှိနိုင်ပါတယ်။

.log

Log file မှာတော့ Vmware ပေါ်မှာ User ပြုလုပ်သမျှ action တွေကို ရရှိနိုင်ပါတယ်။ VM information တွေလဲရရှိနိုင်ပါတယ်။ ဒီလောက်ဆိုဘာတွေ ရနိုင်မလဲ ဆိုတာသိလောက်ပါပြီ။

VMware မှာပါတဲ့ File Type တွေသာမက ကျန်တဲ့ Virtual System တွေက File Type တွေကိုလဲ သိထားသင့်ပါတယ်။

How to Forensics ?

Online Forensic Extraction

Offline Forensic Extraction

Simulation နည်းတွေနဲ့ စစ်ဆေးပါတယ်။

(စစ်ဆေးဖို့အတွက် စစ်ဆေးသူရဲ့ ကျွမ်းကျင်မှု အပြင် ဆက်စပ်အသုံးပြုရမဲ့အရာတွေလဲ လိုအပ်ပါတယ်) တစ်ခုပြောချင်တာကတော့ ဘာတွေပဲသုံးသုံး စစ်ဆေးသူရဲ့ Knowledge က အရေးကြီးဆုံးသောနေရာမှာပါဝင်ပါတယ် ။

Wireless Forensics

Wireless Forensics မှာတော့ အမျိုးမျိုးရှိပါတယ် Bluetooth ကနေပြီးတော့ satellite အထိ အခုဖော်ပြခဲ့အကြောင်းအရာကတော့ Wireless Router Access Point Forensics အကြောင်းပါ။

Wireless Device နှင့်ပတ်သတ်သည်များကို ခွဲခြားခြင်း

ကိုယ် သံသယရှိတဲ့သူ ဖမ်းဆီးရမဲ့သူက Wireless ကို ဘယ်နည်းနဲ့ အသုံးပြုတာလဲ

အခုပေါ်နေတဲ့ Broad Band အမျိုးအစားများ အခြား Wireless Service များ FTTX line များမှ

Wireless Router နှင့်ခွဲဝေခြင်း ဆင့်ပွားပြီးခွဲဝေခြင်း

(repeater.point to point , bridge mode , Client mode), hotspot (Teathering)

စသည်ဖြင့် ဘယ်လိုအသုံးပြုတာကို ခွဲခြားနိုင်ရပါမယ် ။ .

Wireless routers Wireless access points Wireless modems

Wireless network adapters Repeaters Antennas

မှတ်တမ်းတင်ခြင်း

အသုံးပြုသူနှင့်ချိတ်ဆက်ထားသမျှကို video, Photo တစ်ခုခုဖြင့်မှတ်တမ်းတင်ရပါမယ်။

(Adapter , Antenna , Cable ကစ Device အမျိုးအစားအပါအဝင်)

ဘယ်လိုချိတ်ဆက်အသုံးပြုသည်ကို ရှာဖွေမှတ်တမ်းတင်ခြင်း

အပေါ်မှာပြောခဲ့သလိုပဲ ဘယ်နည်းလမ်းနဲ့ အင်တာနက်ကို အသုံးပြုတာလဲ။ point to point , bridge mode , Client mode တို့မှာ တပ်ဆင်ထားပုံကို ဥပမာပြထားပါတယ်။

Wireless signal , channel ,range , Connected Device တို့ကို မှတ်တမ်းတင်ခြင်း

use => window tools (or) Kali wireless hacking tools or Other OS

(MAC SSID Vendor Media type Channel Signal Strength)

ချိတ်ဆက်အသုံးပြုမှုများကို Map ရေးဆွဲခြင်း

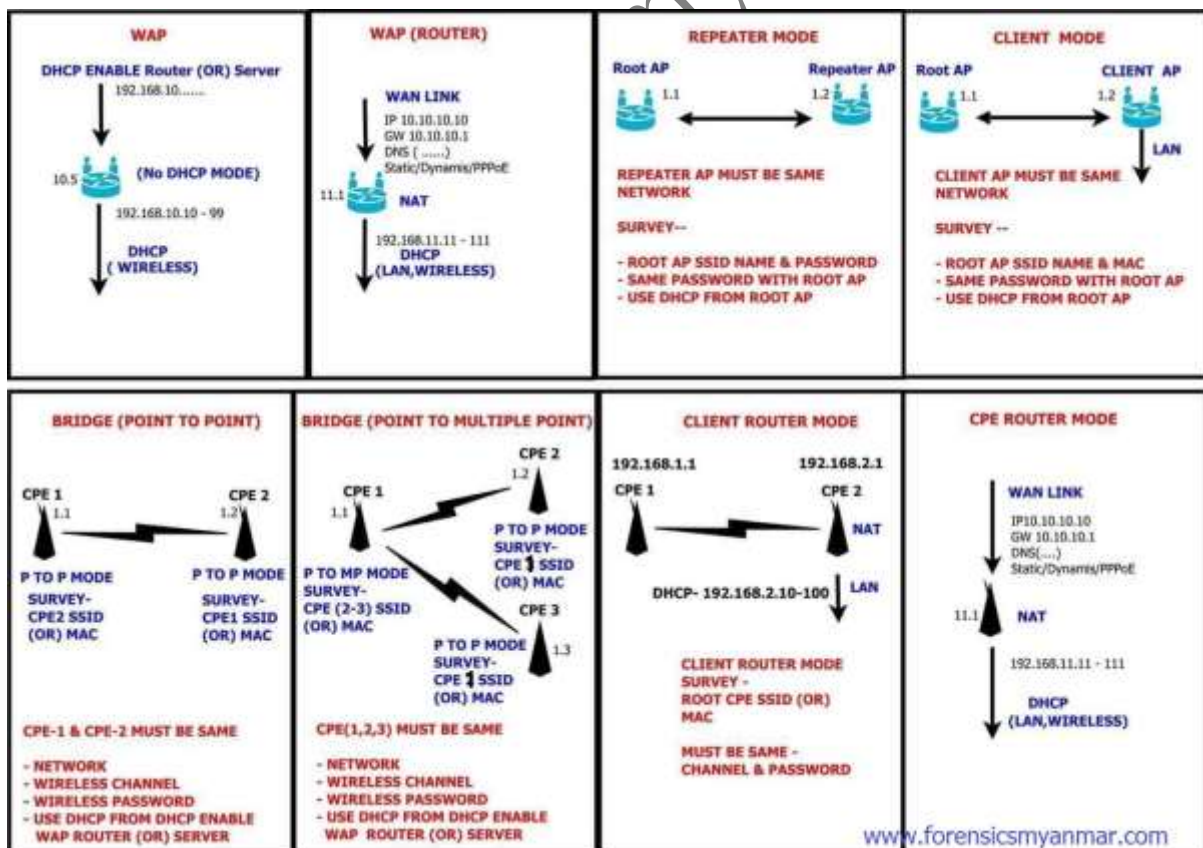
(wireless packet analysis ကတော့ Incident Response အနေအထားမှသာ

ပြုလုပ်တာများသောကြောင့် မဖော်ပြတော့ပါ)

How to Forensics ?

Wireless Network Theory ,Device and Configuration အမျိုးမျိုး တို့ကိုနားလည်မှု, ISP နှင့်ဆက်သွယ်ခြင်း ,

အခြားသော ဆက်စပ်မှုများကို အရင် Post များတွင်ဖော်ပြထားပါသည်။



Event Log Forensics

Event Log ဟာအရေးကြီးသလားဆိုရင် အမှုမထားရင် အရေးမကြီးဘူး အမှတ်ထားရင်တော့ အသုံးလဲဝင်သလို အရေးလဲကြီးပါတယ်။ MS Operation System တစ်ခုလုံးရဲ့ security ကစလို့ software hardware ရဲ့အခြေအနေကိုပြောပြနေတဲ့ Log တွေအားလုံးပါဝင်ပါတယ်။ Forensics သာမက ရိုးရိုး window user တွေရော MS Server သမားတွေအတွက်ပါ အသုံးဝင်ပါတယ်။ အသုံးချနိုင်ရင် incident Response အတွက်ပါ အသုံးဝင်ပါတယ်။

Event Log ကြည့်ပြီးဘာတွေသိနိုင်လဲ

ဘယ် User က ဘယ်အချိန်မှာ ဘာဖြစ်လဲ Remote system တွေကဘာတွေဖြစ်လဲ ဘာတွေကို Access လုပ်သွားလဲ အစရှိသည်ဖြင့်သိနိုင်ပါတယ်။ WS OS အလိုက် MS အလိုက် Version မြင့်လာတာနဲ့အမျှ Event Log file type တွေ file name တွေပြောင်းလာပါတယ်။ ဘာလို့လဲဆို အရင် MS version တွေမှာ file size ကြီးတဲ့အတွက် OS ကို နှေးစေတဲ့အတွက်ပါ။ MS OS vista နဲ့ MS Server 2008 မှာစတင်ပြောင်းလဲလာပါတယ်။

Performance မြန်လာရုံတင်မက log တွေလဲ များစွာပါဝင်လာပါတယ်။

MS Server တွေဆိုလဲ ဒီအတိုင်းပါပဲ။

ပါဝင်တဲ့ Log တွေကတော့သူ့အခွဲတွေ အခွဲတွေအလိုက် အများကြီးပါပဲ။

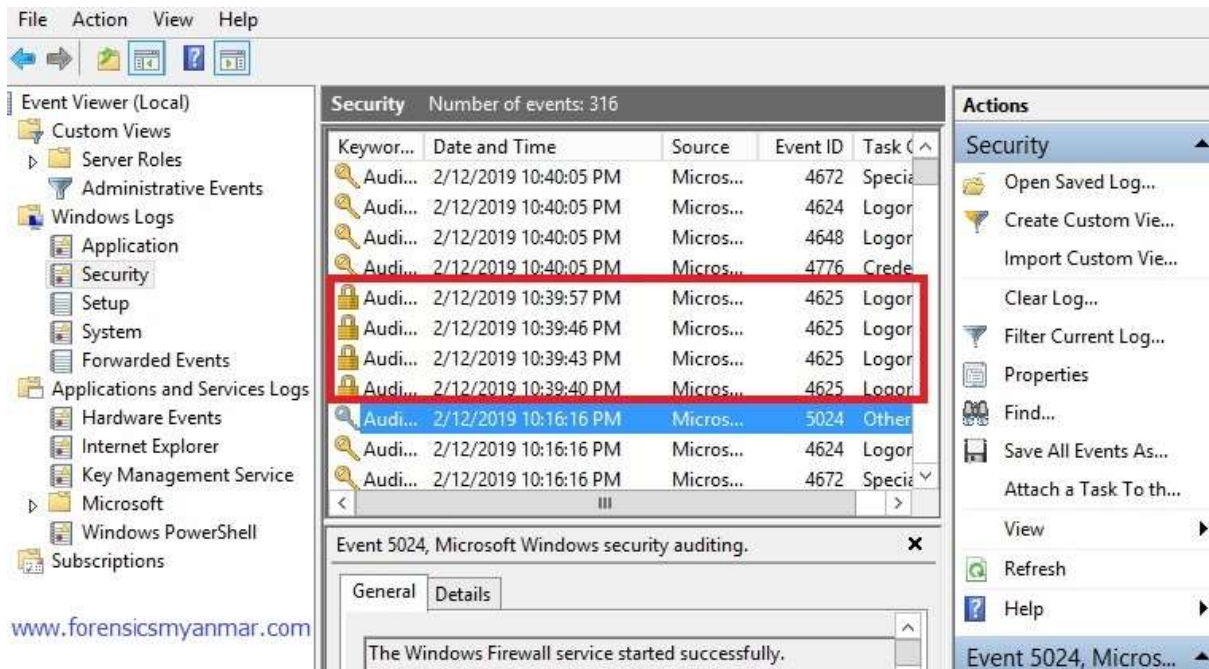
forensics view အရင်ဆိုရင်တော့ case အလိုက်အပြင်ရနိုင်သမျှ Log တွေရနိုင်တာ အကောင်အထုံးပါ။

Case ကရှင်းရင်တော့ log တစ်ခုပဲကြည့်ရုံပါပဲ။

မရှင်းရင် ဆက်စပ်ပြီးတွေးလို့ရအောင်ပါ

MS server မှာဆို subcategory အလိုက်အပိုင်းတွေ ပါဝင်ပါတယ်။

အရေးကြီးတာက အပိုင်းလိုက် အပိုင်းလိုက် (subcategory)ထဲကို ဘာအကြောင်းကြောင့် ဘာဖြစ်လို့ Log တွေဝင်လာတာလဲဆိုတာပါ။



Online (active) live system ကိုတော့ incident Response အတွက်သာ အဓိကထားသုံးတာများပါတယ်။ Offline (System Power Off) အနေအထားမှာလဲ Event Log က investigation လုပ်လို့ရပါတယ်။ ဘာလို့လဲဆိုရင် Event Log က Non-Volatile Information ဖြစ်လို့ပါ။

Power Off သွားရင်လဲ Log ကျန်ပါတယ်။

Event log ဟာ Binary Data Base ဖြစ်တဲ့အတွက် .evt .evtx file extension ဖြစ်ပါတယ်။ Event View ကနေကိုယ်လိုအပ်တဲ့ System Log, Application log , Security log စသည့်ဖြင့် တစ်ခုခြင်း ရွေးပြီး save နိုင်ပါတယ်။ save လို့ရမယ့် File extension တွေကတော့ .evtx .csv .xml .csv တို့ဖြစ်ပါတယ်။

ဖွင့်လို့ရတဲ့ Event View တွေအများကြီးပါ။ အမြင်ရှင်းရှင်းကြည့်လို့ရတာနဲ့ မရတာပဲ ကွာပါတယ်။

Event log file တွေအကုန်ရှိတဲ့နေရာကတော့ C:\Windows\System32\winevt\Logs ဖြစ်ပါတယ်။ နောက်ပိုင်း MS Window , MS Server မှာနေရာတူပါတယ်။

Registry နေရာကတော့

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog

Event Log ကနေ ရနိုင်မဲ့ အချက်အလက်တွေကတော့

Password အပြောင်းအလဲ Time and Date အပြောင်းအလဲ

User logon နဲ့ logout OS start နဲ့ Stop time

User account permission အပြောင်းအလဲ

USB attachment အချက်အလက်တွေ ရနိုင်ပါတယ်။

အရေးပါတဲ့ Event log တွေကတော့

Windows Event log, System Event Log, Security Event Log, Application Event Log, Directory နဲ့ DNS Event Log

MS server မှတော့ log အချို့က သီးခြား enable လုပ်ပေးထားမှသာပေါ်ပါတယ်။ User ကလဲ Log တွေကို မကျန်အောင် disable လုပ်ထားလို့ရပါ

တယ်။ save ယူမဲ့ စက်က System Time မမှန်ရင်လဲ အခက်ခဲရှိပါတယ်။

Computer Name Usernames Date Time တွေလဲ ချိန်းထားနိုင်ပါတယ်။

log တွေကို အခြားနေရာမှာလဲ သိမ်းဆည်းထားတတ်ပါတယ်။

Law Enforcement တွေသာအသုံးပြုနေတဲ့ Forensics tools တွေမှာတော့ investigatorကနေ အချိန်ကုန်အောင် Event view ခေါ် file path တွေ လိုက်ရှာပြီး save စရာ ရှာစရာ မလိုအပ်ပါဘူး ကိုယ်လိုချင်တဲ့ အပိုင်းကိုသာ filter သို့မဟုတ် Click လုပ်ရုံပါပဲ။ တစ်ကယ်တမ်းတော့ Forensics Tools ဆိုတာကလဲ ရှိတဲ့ Open Source တွေရဲ့ အားသာချက်တွေကို ရွေးချယ်ပြီး ပေါင်းစပ်ထားတာပါ။

Event Log forensics ဟာ computer Forensics မှာ အရေးကြီးတဲ့ အစိတ်အပိုင်းမှာ ပါဝင်ပါတယ်။ ဘယ်လို Case ကိုပဲစစ်စစ် နောက်ဆုံး

စစ်ဆေးပြီး ရလဒ်ရေးသားရာမှာ မပါမဖြစ်တဲ့ နေရာကနေပါဝင်ပါတယ်။

The screenshot displays the Windows Event Viewer interface. At the top, two 'DriveImage Verify Results' windows are shown, both indicating a 'Match' for MDS and SHA1 hashes. Below these, the 'Event Viewer (Local)' pane shows the 'USB -INFO' log selected, displaying a list of 75 events. The 'USB -ATTACHMENT' log is also visible, showing 3 events. The bottom pane provides a detailed view of Event 2101, showing a completed Pnp or Power operation for a device.

Level	Date and Time	Source	Event ID	Task Category
Information	2/14/2019 2:00:46 PM	M..	4656	Removable Storage
Information	2/14/2019 2:00:46 PM	M..	4656	Removable Storage
Information	2/14/2019 2:00:46 PM	M..	4656	Removable Storage
Information	2/14/2019 2:00:46 PM	M..	4656	Removable Storage
Information	2/14/2019 2:00:07 PM	M..	4656	Removable Storage
Information	2/14/2019 2:00:07 PM	M..	4656	Removable Storage
Information	2/14/2019 2:00:07 PM	M..	4656	Removable Storage
Information	2/14/2019 2:00:07 PM	M..	4656	Removable Storage
Information	2/14/2019 2:00:07 PM	M..	4656	Removable Storage

Level	Date and Time	Source	Event ID
Information	2/14/2019 3:07:42 PM	DriverFrameworks...	2101

Event Properties - Event 2101, DriverFrameworks-UserMode

General Details

Completed a Pnp or Power operation (27, 20) for device SWD\WPD\BUSENUM\..._T1_UBSTOR\DISK&VEN_UFD_2.0B:PROD_SILICON-POWER16GB&REV_1100#140344980170000001588 (53F56307-B6BF-11D0-94F2-00A0C91EFB8B) with status 0x0.

OPEN SOURCE INTELLIGENCE (OSINT) နှင့် Digital Forensics

Second War ပြီးတဲ့ အချိန်ကနေစပြီး သတင်းမီဒီယာတွေ TV

အစီအစဉ်တွေဟာပိုမိုများပြားလာပြီး ပြောဆိုရေးသာမှု အပိုင်းမှာ ပိုမိုပွင့်လင်းလာခဲ့ပါတယ်။

အဲဒီနောက် Internet ပေါ်လာတဲ့ အချိန်မှာတော့ သတင်းအချက်အလက်စီးဆင်းမှုဟာ

ပိုမိုမြန်ဆန်ကျယ်ပြန့်လာပါတယ်။ ဘယ်နေရာမဆို အဆိုးနဲ့ အကောင်းဒွန်တွဲနေသလိုပါပဲ။

အခုလိုတိုးတက်လာတဲ့အတွက် ကောင်းကျိုးတွေရှိသလို တစ်ဖက်မှာလဲဆိုးကျိုးတွေက

ရှိလာပြန်ပါတယ်။ ဆိုက်ဘာရာဇဝတ်မှု၊ အကြမ်းဖက်အဖွဲ့အစည်း၊ အစိုးရကို

ဝေဖန်တိုက်ခိုက်မှုတွေ စတဲ့အဖွဲ့အစည်းတွေက အင်တာနက်ကို အသုံးပြုကာ

ကျယ်ကျယ်ပြန့်ပြန့်လုပ်ဆောင်လာကြပါတယ်။

Juniper Research အရဆိုရင် လာမဲ့ 2019 မှာ cybercrime ကြောင့် ကမ္ဘာနဲ့တစ်ပုန်းက

စီးပွားရေးလုပ်ငန်းနဲ့ အစိုးရပိုင်းကနေ ကာကွယ်မှုအတွက် ကုန်ကျငွေ ၂ ဘီလီယံခန့်

ရှိမယ်လို့ ခန့်မှန်းထားပါတယ်။ ဒါကြောင့်အစိုးရပိုင်းနဲ့ စီးပွားရေးလုပ်ငန်းကြီးတွေက

ငွေအကုန်ကျသက်သာပြီး တစ်ဖက်တစ်လမ်းကနေ အကျိုးရှိစေမဲ့ Open Source Intelligence

စနစ်ကို အသုံးပြုလာကြပါတယ်။

Open Source Intelligence (OSINT) စနစ်ဆိုတာ ကမ္ဘာအနှံ့မှာ Public ရရှိနိုင်တဲ့

သတင်းအချက်အလက်တွေဖြစ်ပါတယ်။ Open Source Intelligence (OSINT) ဆိုတာကို

ဘယ်နေ့ ဘယ်အချိန်မှာ စတင်ခဲ့ ခေါ်ဝေါ်ခဲ့တယ်ဆိုတာမသိရပေမဲ့ အခုလိုမျိုးနည်းစနစ်ကို

လွန်ခဲ့တဲ့ နှစ်ပေါင်းများစွာထဲက စစ်ရေး စီးပွားရေး နိုင်ငံရေးတွေမှာ အသုံးပြုခဲ့ပါတယ်။ ဥပမာ

အနေနဲ့ အလွယ်ကူဆုံးပြောရရင် ဈေးသတင်းလိုဟာမျိုးပေါ့။ ဈေးသတင်းထဲမှာ

ကုန်ဈေးနှုန်းအတက်အကျ မိသားစုရေး နိုင်ငံရေး ကျမ်းမာရေး စီးပွားရေး သတင်းတွေကို

အခမဲ့ယူနိုင်တဲ့နေရာတစ်ခုပါ။

Internet ခေတ်ရောက်လာတဲ့ အခါမှာတော့ သတင်း website တွေ၊ လူမှုကွန်ယက်တွေ၊

စီးပွားရေး ထုတ်ကုန် ကြော်ငြာတွေ ကနေရယူပါတယ်။ စီးပွားရေးပိုင်းမှာလဲ တစ်ဖက်လုပ်ငန်းက

ဘာတွေလုပ်နေတယ် ဘာထုတ်ကုန်တွေထုတ်နေတယ်ဆိုတာတွေကိုလဲ OSINT နည်းစနစ်တွေနဲ့

ရယူနိုင်ပါတယ်။ Hacking ပိုင်းအတွက်ဆိုရင် Information Gathering အနေနဲ့ Dns lookup , Whois , Ip address Look up , Etc ကနေ အစရှိသည်ဖြင့် ရယူကြပါတယ်။

Social Media ပိုင်းမှာဆို Facebook Graph Search, Twitter Search , Linkedin Search တွေကို အသုံးပြုရင် အသုံးပြုနိုင်သလို အကျိုးများပါတယ်။ အခုလိုရယူခြင်းအတွက် ဥပဒေနဲ့လဲ လွတ်ကင်းသလို ငွေကြေးအကုန်အကျလဲ သက်သာစေပါတယ်။

ငွေကြေးကုန်ကျမှုနည်းပါးသောကြောင့် အထင်သေးသလိုရှိနိုင်ပေမဲ့ လက်တွေ့မှာ နေရာအလိုက် လုပ်ငန်းအလိုက် စနစ်တကျလုပ်နိုင်ရင် အကျိုးများစွာရှိပါသည်။

Open Source Intelligence တွေကိုကြောက်လို့ စစ်ဆင်ရေးနဲ့ လေ့ကျင့်ရေးနေရာတွေမှာ Selfie မဆွဲရ ဓာတ်ပုံမရိုက်ရ အပြင် Electronic Device မယူရ အဆိုတင်သွင်းတာ အောင်မြင်ခဲ့ပါတယ်။

ဆီရီးယားတုန်းက တပ်ဖွဲ့တည်နေရာတွေကို လူမှုကွန်ယက်ကနေ

တစ်ဖက်က ထောက်လှမ်းမိသွားလို့ပါ။

Open Source Intelligence (OSINT) ကိုအများဆုံးနဲ့ အဓိကထားပြီးအသုံးနိုင်ဆုံးကတော့ US နိုင်ငံပါ။ Second war ကာလ မှာရော ယနေ့အချိန်ထိ နိုင်ငံမျိုးစုံ လူမျိုးပေါင်းစုံရဲ့

ဘာသာစကားမျိုးစုံကို တတ်ကျွမ်းနားလည်သူတွေနဲ့စုဖွဲ့ကာ သတင်းအချက်အလက်တွေကို ကုန်ကျမှုနည်းပါးစွာ ရယူနေပါတယ်။ ဥပမာ နိုင်ငံအနှံ့ကသတင်းစာတွေကို ခနထား facebook, Twitter လိုနေရာမျိုးဟာ သတင်းရယူလို့ အကောင်းဆုံးနေရာမျိုးပါ တစ်ကူးတစ်ကကို သတင်းသွားတင် လှုပ်ရှားမှုတွေသွားတင်နေကြပါတယ်။ Hot ဖြစ်တဲ့သတင်းအလိုက် ရေးကြပြောကြသည်။

2008 နောက်ပိုင်းကာလမှာ တပ်မတော်ဘက်က Facebook Twitter Account တွေအပိတ်ခံရသည်။

မြန်မာနိုင်ငံမှာ ဥပမာအနေနဲ့

Operation "Hate Book"

Reuters သတင်းဌာနကနေ Facebook က Hate Speak တွေကို မထိန်းချုပ်နိုင်ဘူး ဆိုတာ သက်သေပြခြင်းတဲ့ အတွက် UC Berkeley School မှာရှိတဲ့ Human Rights Center နဲ့ ပူးပေါင်းပြီး Social media မှာရှိတဲ့ သက်သေတွေကိုရှာတယ်။ အဓိကကတော့ Facebook ထက် မြန်မာနိုင်ငံကို ဦးတည်တာပါ။ Operation အမည်ကတော့ Operation Hate Book ဖြစ်ပါတယ်။

UC Berkeley School (Human Rights Center) မှာ အဓိကပါဝင်သူတွေက Social Network ပိုင်းကျွမ်းကျင်သူတွေ Digital Forensics ကျွမ်းကျင်သူတွေ Human Rights နဲ့ Crime ကျွမ်းကျင်သူတွေပါဝင်ပါတယ်။ အများစုကတော့ Social Media တွေကို ကောင်းကောင်း သုံးနိုင်တဲ့သူတွေပါ။ အဲဒီ Program ကိုတော့ McMahon လို့ခေါ်ပါတယ်။ ဒီ Program အတွက်နှစ်စဉ် လူ 100 ကျော်ကို လေ့ကျင့်ပေးထားပါတယ်။

Facebook , Twitter Graph Search ကို ကောင်းကောင်းအသုံးပြုသွားပါတယ်။

မြန်မာ့အရေးနဲ့ပတ်သတ်သမျှ သတင်းတွေကို online

ကနေရှာဖွေသွားပါတယ်။

သက်ဆိုင်ရာအပိုင်းတွေက နေရလာတဲ့သတင်းတွေ (Screen Shoot) တွေကို Team Leader ကနေ စစ်ဆေးတည်းဖြတ်ပါတယ်။ ပြီးရင် Facebook ကို Report တင်သွားပါတယ်။

Foreign Broadcast Information Service (FBIS) ကဆိုရင် နိုင်ငံပေါင်းစုံက public ကနေအခမဲ့ရနိုင်တဲ့ သတင်းစာနယ်ဇင်းတွေ အင်တာနက် website တွေကနေ အချက်အလက်တွေရယူပြီး ခွဲခြမ်းစိတ်ဖြာအသုံးပြုလျက်ရှိပါတယ်။

OPEN ဖြစ်နေတဲ့ သတင်းတွေ အကြောင်းအရာတွေ ကနေ သတင်းအချက်အလက်ယူတာပါ ...ဒါ တွေယူဖို့ ပိုက်ဆံပေးရလား မပေးရပါဘူး ... ရလာတဲ့ အချက်အလက်တွေကိုခွဲခြမ်းစိတ်ဖြာ အသုံးပြုတတ်ဖို့ပဲလိုတာပါ ...

ဘယ်နေရာမှာ အသုံးဝင်လဲဆိုရင် ကိုယ့် Crush အကြောင်း

စုံစမ်းတဲ့နေရာကနေ ... လူမှုရေး ..စီးပွားရေး နိုင်ငံရေး စစ်ရေး အကြမ်းဖက်နှိမ်နင်းရေး အထိအရေးပါပါတယ်

amazon တို့ကနေ ရောင်းနေနဲ့ စာအုပ် ကိုယ်လဲမဝယ်နိုင်ဘူး ဝယ်လို့လဲအဆင်မပြေ .. ရေးတဲ့အကြောင်း သိလဲသိချင်တယ်... ဘယ်လို အနည်းဆုံးသိနိုင်မလဲ Review နဲ့ မာတိကာ ကနေ သူဘာအကြောင်းတွေရေးမယ် ဘာတွေရေးမယ်ဆိုတာသိနိုင်ပါတယ်...အသေးစိတ်မသိနိုင်ရင် တောင် ခန့်မှန်းလို့ရနိုင်ပါတယ်..OSINT ကိုတစ်ဦးတစ်ယောက်ချင်စီရော အဖွဲ့အစည်း နိုင်ငံအရ ရော . ဉာဏ်စွမ်းရှိသလောက်လုပ်နိုင်ရင် လုပ်နိုင်သလို ရနိုင်ပါတယ်...အဖွဲ့အစည်းလိုက် ခေါင်းစဉ် Sector တွေပြောင်းလဲသွားရုံပါပဲ။

Digital Forensics နဲ့ Countermeasure မှာဆိုရင် ဘယ်နေရာ ဘယ်အချိန်မှာ ဘယ်လိုနည်းနဲ့ တိုက်ခိုက်မှုတွေကြုံရ တယ်။

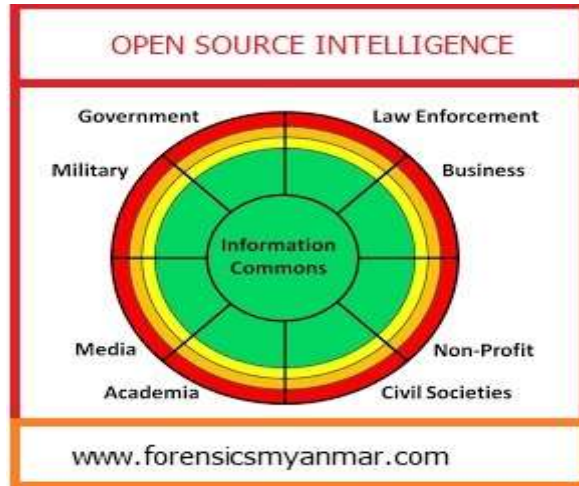
Virus malwares တွေက ဘယ်လိုပုံစံနဲ့ လာတယ်။

အခြားနိုင်ငံတွေ အဖွဲ့အစည်းတွေက Cyber Security အတွက် ဘယ်လိုတွေ့ပြင်ဆင်နေကြတယ်။

Cyber Crime တွေက ဘယ်လိုပုံစံအနေအထားတွေနဲ့ ကျူးလွန်နေကြတယ် ဆိုတာ သတင်းအနေနဲ့ ရရှိနိုင်ပါတယ်။

ကိုယ်မကြုံရပေမဲ့ ကြိုတင်ပြင်ဆင်နိုင်ထောက်လှမ်းစစ်ဆေးနိုင်ပါတယ်။

(တစ်ခုသတိထားရမှာက OSINT ကို Counter လုပ်နိုင်ဖို့ သတင်းအမှားတွေ အတုအယောင်တွေလဲ ထုတ်ပြန်တတ်ပါသည်)



Digital Forensics (48) SCADA(Supervisory Control and Data Acquisition)

အီရန် ညူကလီယား Station ကို တိုက်ခိုက်တဲ့ Stuxnet အကြောင်းကိုတော်တော်များများ သိကြမှာပါ။ Stuxnet က computer ကိုအဓိကထားပြီးတိုက်ခိုက်တာမဟုတ်ပဲ Stuxnet က Computer ထဲကိုရောက်တာနဲ့ Computer မှ PLC စနစ်နဲ့ချိတ်ဆက်ထားခြင်းရှိ ၊ မရှိ ကြည့်ပါတယ်။ PLC က Siemens (PLC) စနစ်ဆိုတာနဲ့ Stuxnet ကစတင်အလုပ်လုပ်ပါတယ်။ Control စနစ်ကို ထိန်းချုပ်တဲ့ Computer ကနေ Control စနစ်ကို အဓိကထားပြီး တိုက်ခိုက်တာဖြစ်ပါတယ်။ အခြားသော Threat တွေလို Threat သက်ရောက်တဲ့ အခါပြသတဲ့ ဖြစ်စဉ်တွေပြသမှာ မဟုတ်ပါဘူး။ Forensics လုပ်ငန်းစဉ်တွေမှာ လုပ်နေတဲ့လုပ်ငန်းစဉ်တွေဟာ (Supervisory Control and Data Acquisition) မှာအသုံးပြုနိုင်ပေမဲ့။ PLC လုပ်ငန်းတွေ ချိတ်ဆက်မှုတွေကို နားလည်နိုင်မှာ မဟုတ်ပါဘူး။ PLC စနစ်ကို ကျွမ်းကျင်သူတွေလိုအပ်ပါတယ်။ များသော အားဖြင့် Control system က အင်တာနက်နဲ့ချိတ်ဆက်ထားခြင်းမရှိပါဘူး။ Social Engineering နည်းကို အသုံးပြုပြီး ဝင်ရောက်တာများပါသည်။ Routeable မလုပ်နိုင်တဲ့ Connection ပေါ်ကနေသွားမယ်ဆိုရင် Forensics လုပ်ဖို့ သီးသန့် Device တွေလိုအပ်ပါတယ်။ Security အရ workstation တွေက အင်တာနက်နဲ့ချိတ်ဆက်ထားတာ နည်းပါးပါတယ်။

Connection ကလဲ Routeable မလုပ်နိုင်တဲ့ Connection နဲ့ပဲသွားပါတယ်။ Monitoring လုပ်ဖို့လဲ ခက်ခဲပါတယ်။

Workstation ဆိုရင်တော့ သုံးထားတဲ့ Window Version အလိုက် Forensics လုပ်နိုင်ပါတယ်။ Live system အခြေအနေမှာ ထိခိုက်မှုအနည်းဆုံးနဲ့ imaging ဒါမှမဟုတ် Event log , Reg Log, Running Process, Memory , opening port တွေကိုယူရပါမယ်။ Volatile အနေအထားအရ SCADA ရဲ့ system status information, LED signal တွေကို နားလည်သူနဲ့ပေါင်းစပ်ပြီး record ယူပါမယ်။ video record ယူတာကအကောင်းဆုံးပါ။ ဓာတ်ပုံဆိုရင် Shutter speed ကြောင့် LED signal တွေအပြောင်းအလဲကို မရယူနိုင်လို့ပါ။ PLC diagram ဆွဲထားတာရှိရင် Future forensics လုပ်ငန်းအတွက် ကူးယူပါ။ SCADA Forensics အပိုင်းတွင် Workstation နှင့် ချိတ်ဆက်မှု အချို့ကလွဲရင် တတ်ကျွမ်းနားလည်သူနှင့် ပူးပေါင်းလုပ်ဆောင်ရပါမည်။

ဖြစ်ပေါ်နေချိန်တွင် Restore Plan လုပ်မလား Forensics Plan လုပ်မလားဆိုတာကတော့ ဖြစ်နေတဲ့အနေအထားအထားပေါ်တွင် များစွာမူတည်ပါသည်။ Restore Plan လုပ်မည်ဆိုလျှင် Forensics အတွက် အခက်အခဲရှိနိုင်ပါသည်။ Forensics လုပ်မည့်အချိန်ကို လက်ရှိအနေအထားက ဘယ်လောက်ကြာကြာထိန်းထားနိုင်မလဲ နှင့် ဘယ်လိုထိခိုက်နစ်နာမှုတွေရှိနိုင်လဲဆိုတာ တွက်ချက်ရပါမည်။

Forensics Process

ဘယ် Device ကို Attack လုပ်တာလဲ

Program bug လား Equipment Fail ဖြစ်တာလား

ဘယ်လို Attack မျိုးလဲ

ဘယ်လိုဖြစ်ပေါ်လာတာလဲ

လက်ရှိစနစ်ထဲမှာရော ရှိနေတုန်းလား

ဘယ်လိုကာကွယ်နိုင်မလဲ

Expert Witness နှင့် Technical Witness

ဒီအပိုင်းကတော့ Forensics Process တွေအကုန်ပြီးတဲ့အချိန်မှာ ပြုလုပ်ရမှာဖြစ်ပါတယ်။ Investigation Report နဲ့အနည်းငယ်ကွဲပြားပါတယ်။ Investigation Report မှာပါတာက Forensics ကို မည်သူက ဘယ်ရက် ကနေ ဘယ်ရက်အထိ ဘယ်လိုနည်းလမ်းနဲ့ ဘာတွေကိုသုံးပြီးစစ်ဆေးတယ်။ စစ်ဆေးတဲ့ထဲက မှ Case နဲ့ပတ်သတ်တာ ဘာတွေတွေ့တယ် မတွေ့ဘူး ဆိုတာကို ရေးသားတာပါ။

Expert Witness ကတော့ မှုခင်းအနေအထားအလိုက် စစ်ဆေးမှုကနေ တွေ့ရှိချက်တွေကို ဥပဒေ လုပ်ထုံးလုပ်နည်းနဲ့အညီ တရားရုံးမှာ ပြောဆိုရတာပါ။ Investigator နဲ့ Expert Witness ကတစ်ဦးထဲလဲ ဖြစ်နိုင်သလို လုပ်ငန်းကျွမ်းကျင်မှုအပေါ်မူတည်ပြီး တစ်ဦးစီလဲ ဖြစ်နိုင်ပါတယ်။ မြန်မာနိုင်ငံမှာတော့ မသိပါ။ အခြားသောနိုင်ငံတွေမှာတော့ တစ်ဖက်ရှေ့နေက Electronic Law နဲ့ IT ပိုင်း နားလည်ရင်နားလည်သလို Investigator , Technical Witness တွေကို ပါ ပြန်လှန်မေးခွန်းထုတ်ပါတယ်။ Technical Witness ဆိုတာကတော့ forensics field မှာ နားလည်သူ တတ်ကျွမ်းသူကို တစ်ဖက်သက်သေပြချက်ဟာ ဟုတ်နိုင်မဟုတ်နိုင် Digital crime ဖြစ်တဲ့ အတွက် တုပလုပ်ဆောင်ထားခြင်းရှိမရှိနဲ့ Electronic Law နဲ့ အခြားသော နိုင်ငံသားရပိုင်ခွင့်ဥပဒေ တွေနဲ့ဆက်စပ်ပြီး မေးမြန်းတာပါ။ Investigator ကိုလဲ စစ်ဆေးပုံကို ဥပဒေ ရပိုင်ခွင့်နဲ့ အညီ စစ်ဆေးပုံစစ်ဆေးနည်းတွေ ကိုပါ အသေးစိတ်မေးမြန်းပါတယ်။ များသားအားဖြင့် Expert Witness တွေဟာ Law နဲ့

ပတ်သတ်တာတွေကို နားလည်တတ်ကျွမ်းသူတွေ၊ IT ပိုင်းဆိုင်ရာ နားလည်တတ်ကျွမ်းသူတွေဖြစ်ပါတယ်။ တစ်နည်းအားဖြင့် တရားရုံးနဲ့ပတ်သတ်သော အတွေ့အကြုံရှိရမှာ ဖြစ်ပါတယ်။ အဓိက အချက်ကတော့ ပြစ်မှု ရှိတယ် မရှိဘူး ဆိုတာကို အခြားသော မှုခင်းမှာပါဝင်တဲ့ သက်သေခံချက် အပေါ်မှာ အထောက်အကူဖြစ်ရပါမယ်။ Expert Witness ဟာ Lawyer မဟုတ်ပါဘူး။ ပြန်လှန်မေးခွန်းတွေ ၊ လိုပြ

သက်သေတွေနဲ့ပတ်သတ်တဲ့မေးခွန်းတွေ အဖြေတွေကိုရှေ့နေကိုအကြံပေးခြင်းဖြစ်ပါတယ်။

ပြည်ပနိုင်ငံတွေမှာတော့ Witness တစ်ဦးမှာ ရှိရမဲ့ အရည်အချင်းတွေကို သတ်မှတ်ထားပါတယ်။ ဥပမာ အတန်းပညာ၊ ဥပဒေအတွေ့အကြုံ ၊ IT ပိုင်းဆိုင်ရာ Certificate၊ သင်ကြားရေးအတွေ့အကြုံ၊ စာအုပ်စာတမ်းထုတ်ဝေမှု

Foreneics ပိုင်းဆိုင်ရာသင်တန်းပြီးမြောက်အခြားသောမှု စတာတွေနဲ့သတ်မှတ်ထားပါတယ်။ နိုင်ငံရေးပါတီ၊ ရှေ့နေများ Law Firm လုပ်ငန်းများနဲ့ပတ်သတ်ကြောင်းနဲ့လဲ သတ်မှတ်ပါတယ်။

Investigator တွေရဲ့ ပညာအရည်အချင်း၊ IT ပိုင်းဆိုင်ရာ Certificate၊ ဒါ့အပြင် စစ်ဆေးတဲ့ Forensics Tools , Device အလိုက် Certificate တွေကို မေးမြန်းသလို၊

တစ်ဖက်ရှေ့နေက တရားရုံးမှာလဲ တင်ပြရပါတယ်။

တစ်ဖက်ရှေ့နေမှာ Technical Expert ရှိရင် သက်သေ

အဖြစ်ခေါ်ယူပြီး စစ်ဆေးပုံ စစ်ဆေးနည်းကိုပါ investigator အားမေးမြန်းတာတွေလုပ်ပါတယ်။

မြန်မာနိုင်ငံမှာ Example အနေနဲ့ကြည့်မယ်ဆိုရင်

ရိုက်တာ သတင်းထောက်နှစ်ယောက်အမှုတွင် တရားခံရှေ့နေဘက်မှ မေးမြန်းမှု) (Irrawady သတင်းဌာနမှ English New အဖြစ်ရေးသားထားပါသည်။။

မြန်မာဘာသာဖြင့်ရေးသားထားခြင်းမတွေ့ရပါ)

(Digital Forensics Version - 1.1)

ThirdEye

IoT Device Forensics Flow

IoT Device တွေဟာ 2020 မှာ 34 ဘီလီယံခန့်ရှိလာနိုင်ပါတယ်။ Digital Forensics ထဲမှာ IoT forensics အပိုင်းပါဝင်ပေမဲ့ နည်းပညာပိုင်းအရ အသုံးပြုတဲ့ Hardware ပိုင်းအရ ကွဲပြားခြားနားပါတယ်။ Iot မှာ cable,wireless,RF,Bluetooth,Sensor နဲ့ application မျိုးစုံပါဝင်ပါတယ်။ digital Forensics မှာအသုံးပြုတဲ့စုံစမ်းစစ်ဆေးရေးနည်းနဲ့ အသုံးပြုတဲ့ပစ္စည်းတွေကကွဲပြားမှုရှိပါတယ်။ အသုံးပြုတဲ့အနေအထားSensor တွေနဲ့ပတ်သတ်ပြီး Iot device မျိုးစုံရှိပါတယ်။ ဒါကြောင့် Iot device ကို သီးသန့်စစ်ဆေးတဲ့ Forensics device တွေ tools တွေအရမ်းနည်းပါးပါတယ်။ Case တစ်ခုဖြစ်ရင် Iot device အလိုက်ကျွမ်းကျင်တဲ့ ပညာရှင်သီးသန့်လိုအပ်သလို သူ့ရဲ့ထင်မြင်ယူဆချက်ကလဲ အရေးကြီးပါတယ်။

IoT Forensics Flow မှာ လုပ်ဆောင်ရမဲ့ အပိုင်းတွေ ဆက်စပ်စဉ်းစားရမဲ့ အပိုင်းတွေရှိပါတယ်။

Case အပေါ်မူတည်ပြီးဖော်ထုတ်ခြင်းအပိုင်းနှင့် ဆက်စပ်စဉ်းစားခြင်း

အခင်းဖြစ်တဲ့ နေရာမှာရှိတဲ့ IoT device ကဘယ်လိုအမျိုးအစားလဲ ဘာအတွက်သုံးတာလဲဆိုတဲ့အပိုင်း

Iot device နဲ့ ဘာတွေကို ဘယ်လိုချိတ်ဆက်ထားလဲဆိုတဲ့အပိုင်း

Iot Device တွေကို ဘာနဲ့အဓိကထိန်းချုပ်သလဲဆိုတဲ့အပိုင်း

ထိန်းချုပ်တဲ့ Device နဲ့ Iot Device နဲ့ ဘယ်လို ဆက်သွယ်သလဲဆိုတဲ့အပိုင်း

(တိုက်ရိုက်ဆက်သွယ်တာလား ကြာခံ medium device သုံးသလား eg-wireless router)

မူခင်းမဖြစ်ခင်အချိန်မှာ ဘာတွေရှိလဲ ဘာတွေဖြစ်လဲ

မူခင်းဖြစ်တဲ့အချိန်မှာ ဘာတွေရှိလဲ ဘယ်သူတွေရှိလဲ

(Iot device အများစုဟာ communication အတွက် wireless,bluetooth ကိုအဓိကထားသုံးပါတယ်)

Iot devie ကနေ တပ်ထားတဲ့ Sensor နဲ့ program အရပြောင်းလဲမှုကို ထိန်းချုပ်သူကသိရှိနိုင်သလား မသိရှိနိုင်ဘူးလား

Iot Device အပြင် ဆက်သွယ်ထားတဲ့ Device တွေ sensor တွေရဲ့ Data တွေက ဘယ်နေရာမှာ

ဘယ်လို file type နဲ့ Save ထားတာလဲ

IoT device တွေနဲ့ ဆက်စပ်သမျှ အားလုံးကို စစ်ဆေးဖို့လိုအပ်သလား

ကျွမ်းကျင်သူမပါပါက အကုန်စစ်ဆေးဖို့လိုအပ်ပါမယ် (သိမ်းဆည်းခြင်းလဲအတူတူပါပဲ)

(သိမ်းဆည်းခြင်းအပိုင်းကတော့ မှုခင်းအခြေအနေနဲ့ ဥပဒေအတိုင်းသာဖြစ်သည်)

သတိထားရမဲ့ အချက်တွေတော့ရှိပါတယ်။ သိမ်းဆည်းရမဲ့ IoT device ကို မူလအခြေအနေမပျက်သိမ်းဆည်းဖို့ရနိုင်မလား ? Data တွေကဘယ်နေရာမှာ save ထားလဲနဲ့ Device ရဲ့သဘောသဘာဝအပေါ်မူတည်ပါတယ်။ ပါဝါဖွင့်ထားပြီး သိမ်းဆည်းမလား ? ပိတ်ပြီးသိမ်းလိုက်ရင် ဘာတွေထိခိုက်သွားနိုင်မလဲ ? First Responder team မှာ Data Collect လုပ်ဖို့ ဘာတွေပါလာသလဲ ? ထိန်းသိမ်းဖို့ရောဘာတွေပါလာသလဲ ?

အပူချိန် အသံ လှုပ်ရှားမှု လက်ဇွေ SENSOR တွေပါ ပါနေတဲ့အခါမှာ သိမ်းဆည်းရင် အခြေအနေပြောင်းလဲနိုင်သလား ? ပုံကြမ်းမရရင်တောင် ဓာတ်ပုံအရယူရပါမယ်

(LAB တစ်ခုစမ်းဖို့ ကျွမ်းကျင်သူနဲ့တိုင်ပင်ထားပါတယ် စမ်းသပ်ပြီးရင် အခြေအနေပြန်တင်ပေးပါမယ်)

စစ်ဆေးခြင်းအပိုင်း

သိမ်းဆည်းသူထံမှရတဲ့ ပုံစံအကြမ်း (Eg. Network Diagram) အတိုင်း Iot နဲ့ ဆက်စပ်တဲ့ ပစ္စည်းတွေကို ပုံစံချကြည့်ရပါမယ်။ ပုံကြမ်းမရင် ကျွမ်းကျင်သူနဲ့ သိမ်းဆည်းတဲ့ device တွေအတိုင်း ပုံစံချကြည့်ရပါမယ်။

ဒါမှ စစ်ဆေးတဲ့အခါမြင်သာမှုရှိမှာပါ။

သက်ဆိုင်ရာ IoT Device အနေအထားပုံစံအလိုက် ကျွမ်းကျင်သူလိုအပ်ပါတယ်။ ပြည်တွင်းဖြစ်မဟုတ်ပဲ smart home security လိုဟာမျိုးဆိုရင်တော့ Google တော့ခေါက်ရပါမယ်။ဒါမှ device ကိုဘယ်လိုအသုံးပြုသလဲ အသုံးပြုသလဲ

Manual guide ကဘာလဲဆိုတာသိနိုင်မှာပါ

Data Communication , Remote Control အပိုင်းအတွက် Network Forensics ကျွမ်းကျင်သူလိုအပ်ပါတယ်။

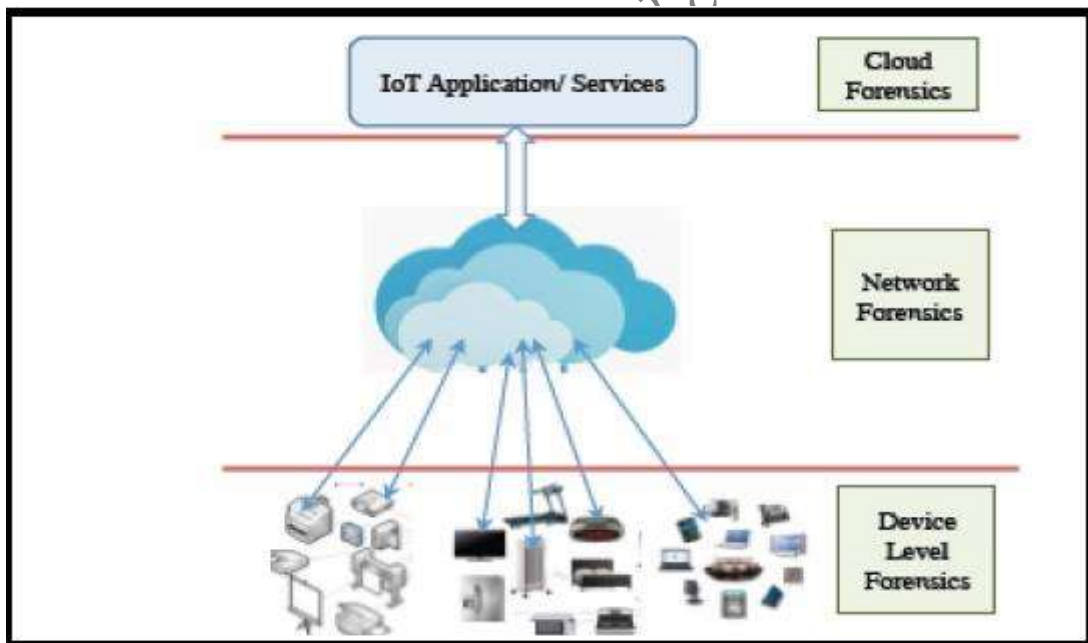
Data storage အပိုင်းအရ Storage ပိုင်းကျွမ်းကျင်သူ Cloud ပိုင်းကျွမ်းကျင်သူလိုအပ်ပါတယ်။ IoT Device ကိုControl လုပ်နိုင်တဲ့ Device အလိုက် ကျွမ်းကျင်သူလိုအပ်ပါတယ်။ Eg . Mobile Phone or Tablet

တရားရုံးတင်တဲ့အပိုင်းနဲ့ လျှောက်လဲခြင်းအပိုင်းကတော့ မလိုအပ်တဲ့အတွက်မရေးတော့ပါဘူး

ပုံထဲမှာတော့ ဆက်စပ်စဉ်းစားရမဲ့ အပိုင်းကို ရေးပေးထားပါတယ်။

အသစ်အသစ်ထွက်လာတဲ့ Iot Device တွေ ဥပဒေအရလုပ်ပိုင်ခွင့်တွေ ငွေကြေးနဲ့ လူသားအရင်းအမြစ် အရ Iot Forensic အပိုင်းဟာ စိန်ခေါ်မှုများစွာရှိနေမှာပါ

IoT (Internet of Things) Forensics	
What Happen ?	When did it happen ?
How did it happen ?	Who and or What did it ?
Why Did it happen ?	What data was collected ?



NTFS File System timestamp Forensics

NTFS file system ထဲမှာ Master File Table (MFT)ပါဝင်ပါတယ်။ HardDisk အကြောင်းရေးသားတုန်းက MFT ထဲမှာ Hard Disk ရဲ့ ဘယ် Cluster ဘယ်လောက်မှာတော့ file ,folder နဲ့ပတ်သတ်တဲ့ အချက်အလက်တွေ ကို သိမ်းထားပါတယ်ဆိုပြီး ဖော်ပြခဲ့ပါတယ်။MFT မှာ နောက်ထပ်သိမ်းထားတာကတော့ **MFT ရဲ့ \$STANDARD_INFO ထဲမှာ**

Modified Time (M-time)

Accessed Time (A-time)

Created Time (C-time)

Changed (\$MFT မှာ Modifiedလုပ်တဲ့အချိန်)

(သာမန်အနေအထားဖြင့် User မမြင်နိုင်)

ဆိုပြီး 4 ခုရှိပါတယ်။ အပေါ် 3 ခုဖြစ်တဲ့ Modified Time (M-time) Accessed Time (A-time) Created Time (C-time) ကတော့ user ကကြည့်လို့ရပါတယ်။ Changed (\$MFT Modified) ကိုတော့ Forensics tools တွေ MFT viewer tools တွေနဲ့ကြည့်လို့ရပါတယ်။ example autopsy, Encase,FTK,

\$FILE_NAME မှာတော့ file, folder တွေရဲ့အမည်ကို မှတ်သားထားပါတယ်။

ဒါဆိုရင် file တစ်ခု folder တစ်ခုကိုကြည့်တာနဲ့ ဘယ်အချိန်မှာ Create လုပ်တယ်ဘယ်အချိန်မှာ modified (edit) လုပ်တယ် ဘယ်အချိန်မှာ access လုပ်တယ်ဆိုတဲ့ MAC time ကိုသိနိုင်ပါတယ်။ Antiforensics အနေနဲ့ time stamp ကိုပြင် နိုင်ပါတယ်။ file folder တွေကို တစ်ခုချင်းစီအလိုက် ပြင်သလို file folder အားလုံးကို random ချပြီး timeတွေအကုန်ပြောင်း လိုက်တာလဲဖြစ်နိုင် ပါတယ်။ Example timestomp

timestamp ကိုစစ်ဆေးတဲ့အခါ သာမန်စစ်ဆေးတဲ့အနေအထားမှာရော timestamp (antiforensics) ဖြစ်တဲ့အခါမှာရော စဉ်းစားရမည့်အချက်တွေကတော့ W5 မေးခွန်းပဲဖြစ်ပါတယ်။

what ? File ကဘာအမျိုးအစားလဲ

Where? File က ဘယ်နေရာမှာရှိတာလဲ

Why ? file ကဘာလို့ ဒီနေရာမှာရှိနေရတာလဲ

How ? ဘယ်လိုရောက်လာတာလဲ

Who? ဘယ်သူက လာထားတာလဲ

Text File ကိုစမ်းသပ်ထားရာမှာတော့ Win 10 မှာ hello.txt ကို time zone မတူတဲ့ ကွန်ပျူတာ W7 မှာပြောင်းလိုက်တဲ့ အနေအထားကတော့ပြောင်းလဲမှုရှိတာကို တွေ့ရမှာဖြစ်ပါတယ်

Properties	
Name	Hello.docx
S	NO_SCORE
C	NO_COMMENT
O	-1
Location	/img_01.001/Hello.docx
Modified Time	2019-04-17 19:49:09 MMT
Change Time	2019-04-17 21:07:46 MMT
Access Time	2019-04-17 19:49:09 MMT
Created Time	2019-04-17 19:48:49 MMT

MCAB Time

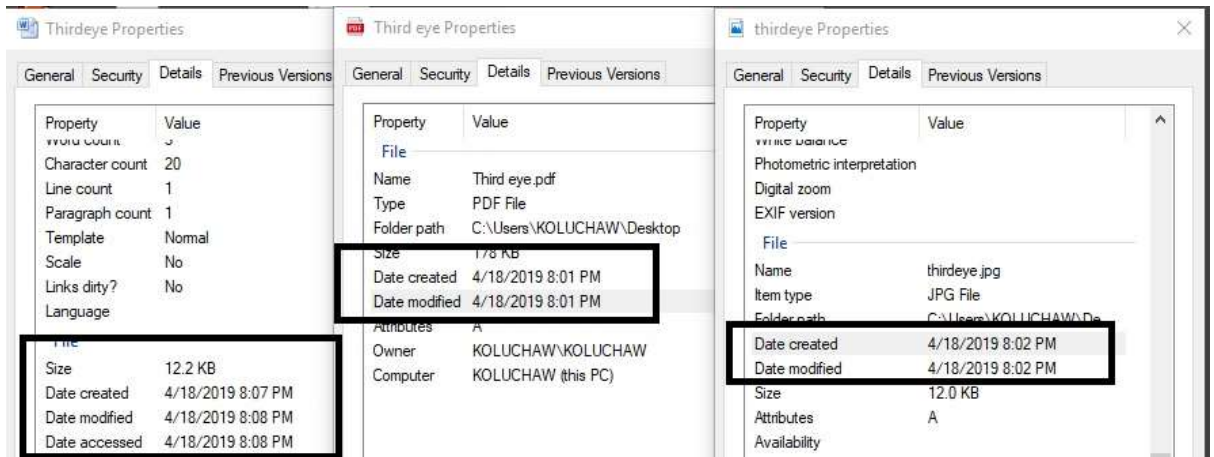
hello Properties	
General Security Details Previous Versions	
Property	Value
File	
Name	hello.txt
Type	Text Document
Folder path	C:\Users\KOLUCHAW\Desktop
Size	18 bytes
Date created	4/17/2019 10:04 PM
Date modified	4/17/2019 10:04 PM

window 10 တွင် txt file create လုပ်ထားခြင်း

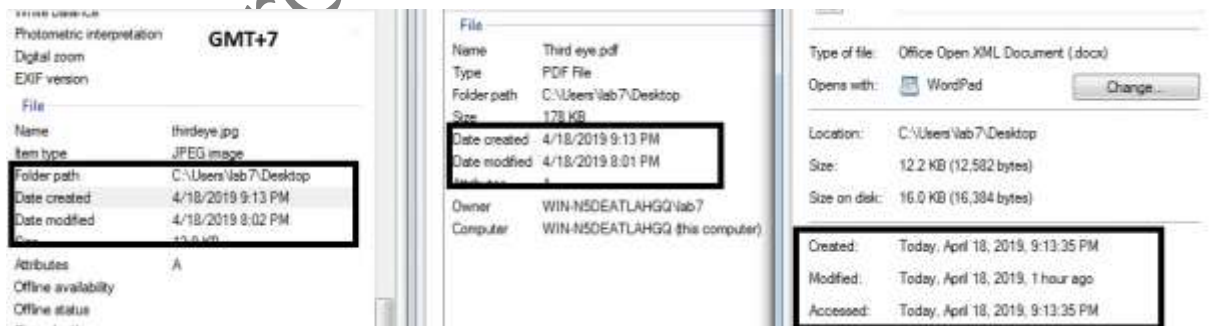
hello Properties	
General Security Details Previous Versions	
Property	Value
File	
Name	hello.txt
Type	Text Document
Folder path	C:\Users\lab7\Desktop
Size	49 bytes
Date created	4/17/2019 10:46 PM
Date modified	4/17/2019 10:47 PM

W10 မှ window 7 သို့ txt file ပြောင်းထားလိုက်သောအခါ

NTFS Time Stamp Forensics ကိုထပ်စမ်းသပ်ကြည့်ရအောင်ပါ။ w10 မှာ thirdeye အမည်နဲ့ word, pdf, image file 3 ခု create လုပ်ထားလိုက်ပါတယ်။ timezone က GMT6:30 အချိန်နဲ့ပါ။ file တစ်ခုချင်းစီရဲ့ metadata timestamp ကို ပုံမှန်ကြည့်နိုင်ပါတယ်။



အခုအချိန်မှာ window 10 u thirdeye အမည်နဲ့ word, pdf, image file 3 ခုကို Window 7 (GMT7) ထဲကို ပြောင်းထည့်လိုက်ပါတယ်။ file တစ်ခုချင်းစီရဲ့ metadata , timestamp မှာ အောက်ပါအတိုင်းပြောင်းလဲသွားတာ တွေ့နိုင်ပါတယ်။



ဒါကြောင့် TimeZone လွဲနေတဲ့ GMT 7 နဲ့ window 7 ကို Time Zone ပြောင်းပြီးလေ့လာကြည့်ပါမယ်။ အခုအနေအထားမှာ window 7 က vmdk file type ဖြစ်ပါတယ်။ vmdk file type ဖြစ်လို့ vmware ကို disk image (bit by bit) Copy ယူပါမယ်။ Logical Drive တစ်ခုလုံးအစား အခုအချိန်မှာ vmdk

တစ်ခုကိုပဲ image ယူထားပါတယ်။ မစစ်ဆေးခင်မှာ forensics လုပ်တဲ့ workstation timezone သို့မဟုတ် forensics tools ရဲ့ timezone ကိုချိန်းထားရပါမယ်။ Example Encase , autopsy, FTK Thirdeye ဆိုတဲ့ World file က forensics workstation မှာပြောင်းလဲသွားပုံပါ

```
MFT Entry Header Values:
Entry: 41969      Sequence: 3
$LogFile Sequence Number: 190107368
Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 602 (S-1-5-21-1473477398-30105749-947339880-1000)
Last User Journal Update Sequence Number: 23964112
Created:      2019-04-18 20:43:35.647176900 (Myanmar Standard Time)
File Modified: 2019-04-18 19:38:34.000000000 (Myanmar Standard Time)
MFT Modified:  2019-04-18 20:43:35.647176900 (Myanmar Standard Time)
Accessed:      2019-04-18 20:43:35.647176900 (Myanmar Standard Time)
```

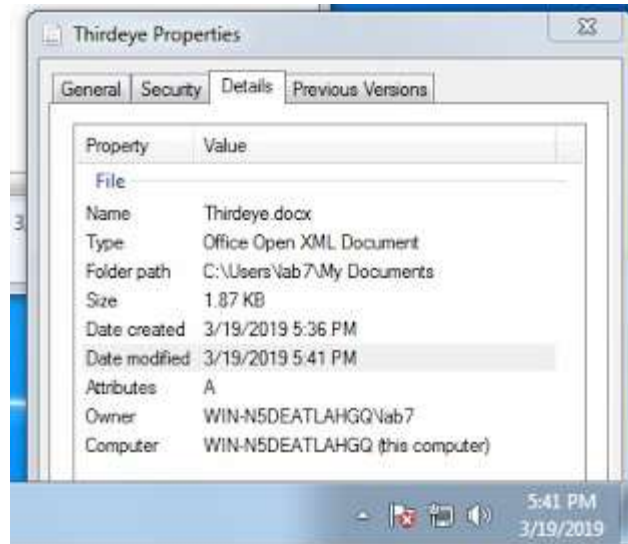
Thirdeye.World file ရဲ့ Metadata တွေပါ

```
MFT Entry Header Values:
Entry: 41969      Sequence: 3
$LogFile Sequence Number: 190107368
Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 602 (S-1-5-21-1473477398-30105749-947339880-1000)
Last User Journal Update Sequence Number: 23964112
Created:      2019-04-18 20:43:35.647176900 (Myanmar Standard Time)
File Modified: 2019-04-18 19:38:34.000000000 (Myanmar Standard Time)
MFT Modified:  2019-04-18 20:43:35.647176900 (Myanmar Standard Time)
Accessed:      2019-04-18 20:43:35.647176900 (Myanmar Standard Time)
```

Case Back Ground (example)

Company တစ်ခုမှ အကြီးတန်း ဝန်ထမ်းတစ်ဦးက company ကနေအလုပ်ရပ်စဲခြင်းခံရပါတယ်။ အလုပ်ကမထွက်ခင် company မှ အရေးကြီး file တစ်ခုကို ရည်ရွယ်ချက်တစ်ခုနဲ့ ယူဆောင်သွားပါတယ်။ဆက်ပြီး အပြင်မှာ ပြန်လည်ရောင်းချခြင်းပြုလုပ်ပါတယ်။ အရင်ကလုပ်ထားသမျှကို ကွန်ပျူတာထဲမှာ မထားရှိရဘူးဆိုတဲ့ လက်မှတ်လဲရေးထိုးထားပါတယ်။စစ်ဆေးတဲ့အချိန်မှာ ကွန်ပျူတာက clock ကို backdate ပြုလုပ်ထားပါတယ်။



Back Date ပြုလုပ်ထားပုံ

Methodology နဲ့ Hypothesis အပိုင်းကပျင်းစရာကောင်းတဲ့အတွက်ချန်လှုပ်ထားခဲ့ပါတယ်။စစ်ဆေးတဲ့ခါ I nternet History ,User ,Create time, USB history, နဲ့ System ကိုစစ်ဆေးတဲ့အခါမှာ window time ကို back သို့ပြောင်းထားကြောင်းသိသာစွာတွေ့ရမှာဖြစ်ပါတယ်။

```

Entry: 40889      Sequence: 2
$LogFile Sequence Number: 186986957
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 562 (S-1-5-22-544)
Last User Journal Update Sequence Number: 20389016
Created:      2019-04-15 00:32:43.878881500 (MMT)
File Modified: 2019-04-14 17:25:31.606808400 (MMT)
MTT Modified: 2019-04-14 17:25:31.606808400 (MMT)
Accessed:     2019-04-14 17:25:13.182754600 (MMT)

$FILE_NAME Attribute Values:

```

```

Name: /img_Windows 7 vmdk/vm1_vs2/Windows/System32/config/RegBack/SOFTWARE
Type: File System
MIME Type: application/octet-stream
Size: 21594112
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2019-04-14 17:25:10 MMT
Accessed: 2019-04-14 17:23:14 MMT
Created: 2019-04-15 00:32:43 MMT
Changed: 2019-04-14 17:25:10 MMT

```

Name	/img_Windows 7.vmdk/vol_vol2/Windows/System32/config/RegBack/SOFTWARE
Type	File System
MIME Type	application/octet-stream
Size	21594112
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2019-04-14 17:25:10 MMT
Accessed	2019-04-14 17:23:14 MMT
Created	2019-04-15 00:32:43 MMT
Changed	2019-04-14 17:25:10 MMT

File System တစ်ခုမှာ Categories 5 ခု ရှိတယ်လို့သတ်မှတ်နိုင်ပါတယ်။ Digital Forensics လုပ်တဲ့နေရာမှာရော သက်သေခံတင်ပြတဲ့နေရာမှာရော ယခုဖော်ပြထားတဲ့ Categories 5ခုစလုံးက အကျိုးဝင်ပါတယ်။

File System (Eg.NTFS,FAT32,)

File Content (Eg.docx .txt,.html)

Metadata (Eg. file location, Time Stamp)

File Name (Name of file)

Application (Eg. File Open Application , MS Word, WordPad and Notepad)

NTFS မှာ docx file တစ်ခုကို ပြုလုပ်ပြီး Copy,Cut လုပ်ကာ မတူတဲ့ Location တွေမှာ ထားကြည့်တာပါ။ Create Date (ctime) ကပြောင်းလဲမှုမရှိတာကိုတွေ့ရမှာဖြစ်ပါတယ်။

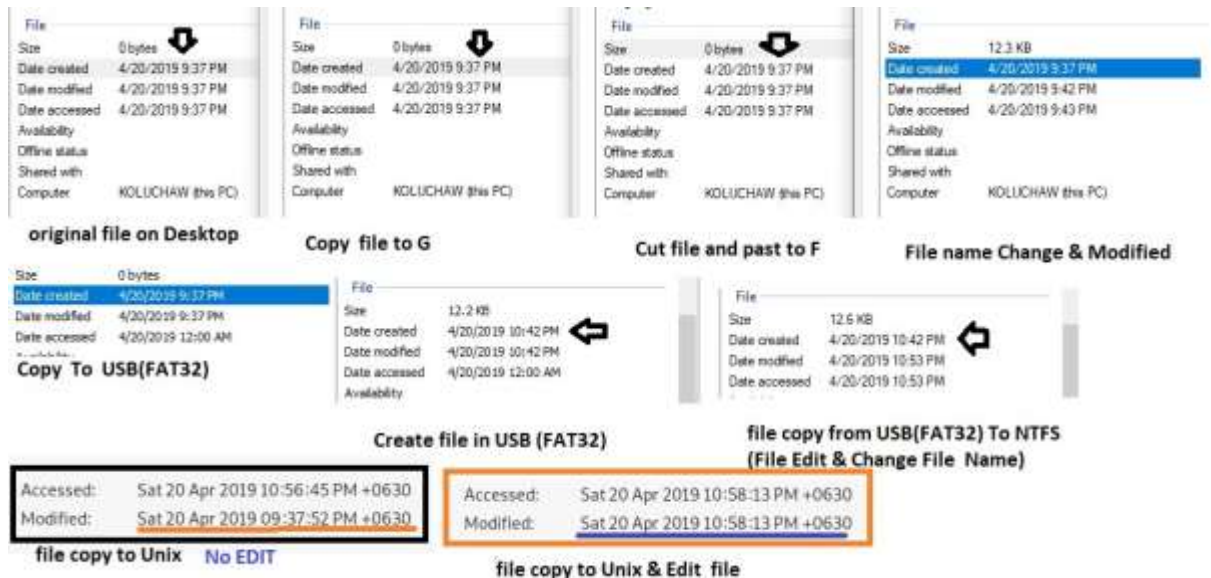
နောက်ထပ် FAT32 (USB) ထဲကိုပြောင်းလဲကြည့်တဲ့အခါမှာလဲ (ctime) ကပြောင်းလဲမှုမရှိတာကိုတွေ့ရမှာဖြစ်ပါတယ်။FAT32 မှာ Last Accessed Date time ကိုမှတ်သား ထားခြင်း မရှိပါ။ Create Date & Times, Modify Date & Times ကိုသာမှတ်သားထားပါတယ်။

FAT32 (USB)ထဲမှာ docx file တစ်ခုကိုပြုလုပ်ပြီး NTFS ထဲကို ပြောင်းထည့်တဲ့အခါမှာလဲ(ctime) ပြောင်းလဲမှုမရှိတာကိုတွေ့ရမှာဖြစ်ပါတယ်။

NTFS ထဲမှာပဲ ခုနက paste လုပ်ထားတဲ့ File ကို File Name ပြောင်းပြီး အထဲက စာတွေ Edit လုပ်တဲ့ အခါမှာလဲ (ctime) ပြောင်းလဲမှုမရှိတာကို တွေ့ရမှာဖြစ်ပါတယ်။

နောက်ထပ် EXT4 (Kali) ထဲကို ခုနက docx file ကိုပြောင်းထည့်လိုက်ပါတယ်။ Open,Edit မလုပ်ပါဘူး။ အဲဒီအခါမှာ Modified Date ကပြောင်းလဲသွားပြီး Accessed Date မှာ ပြောင်း လိုက်တဲ့ အချိန်ကိုဖော်ပြနေတာတွေ့ရမှာဖြစ်ပါတယ်။

EXT4 ထဲမှာ ခုနကပြောင်းထည့်လိုက်တဲ့ docx file ကို Edit ,File Name ပြောင်းလိုက်တဲ့အခါမှာ Accessed Date နဲ့ Modified Date ဟာ EXT4 (Kali) မှာရှိတဲ့ Time Zone အတိုင်းပြောင်းလဲ သွားတာကို မြင်ရမှာဖြစ်ပါတယ်။



Unix(Linux) System မှာအများဆုံးအသုံးပြုနေတဲ့ အစောပိုင်း EXT4 System မှာတော့

Access Time (atime)

Change Time (ctime)

Modify Time (mtime) ကိုမှတ်သားထားပါတယ်။

File Creation Time ကိုမှတ်သား ထားခြင်းမရှိပါဘူး။ Access Time (ctime) နဲ့ Modify Time (mtime) တို့က ထပ်တူညီနေရင် File Creation Time အဖြစ်သာမှတ်ယူနိုင်ပါတယ်။File တစ်ခုကို create လုပ်လိုက်တာနဲ့ atime, time , mtime တွေက Current Time အနေဖြင့်သာပြသပါတယ်။ နောက်ပိုင်း EXT4 System မှာတော့ Create Time (Birth Time) ကိုပါပြသပါတယ်။

Access Time (ctime) ဆိုတာကတော့ Unix(Linux) တစ်ခုမှာ CLI Or GUI ကနေ File တစ်ခုကို (read) လုပ်တဲ့ နောက်ဆုံးအချိန်ကိုဖော်ပြတာဖြစ်ပါတယ်။ နေရာတစ်ခုကို ပြောင်းလိုက်တဲ့အချိန်ကိုလဲ Access Time (ctime) နဲ့ပြပါတယ်။ ပြောင်းလဲမှုကို Current Time နဲ့ပြသပါ တယ်။

Change Time - (ctime) ကိုတော့ file တစ်ခုကို Ownership , Access Permissions စတာတွေချိန်းလိုက်တဲ့ အချိန်မှာ ပြသပါတယ်။

Modify Time - (mtime) ကို File တစ်ခုရဲ့ Content ကိုချိန်းတဲ့အချိန်ကိုပြသပါတယ်။(eg. edit and Save)

```
root@kali:~# ls -l UNIX-1
-rwxrwxrwx 1 root root 36 Apr 21 06:38 UNIX-1
root@kali:~#
root@kali:~# cp UNIX-1 /etc/
root@kali:~# ls -l /etc/UNIX-1
-rwxr-xr-x 1 root root 36 Apr 21 06:36 /etc/UNIX-1
root@kali:~#
```

Accessed Time (atime)

```
root@kali:~# stat UNIX-1
File: UNIX-1
Size: 114          Blocks: 8          IO Block: 4096
Device: 801h/2049d Inode: 186002    Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (  0/   root)
Access: 2019-04-21 06:38:51.951529109 +0630
Modify: 2019-04-21 06:38:51.951529109 +0630
Change: 2019-04-21 06:38:51.951529109 +0630
Birth: -
```

atime,ctime,mtime

```
root@kali:~# chmod 755 UNIX-1
root@kali:~# ls -lc UNIX-1
-rwxr-xr-x 1 root root 36 Apr 21 06:38 UNIX-1
root@kali:~# vi UNIX-1
root@kali:~# ls -lu UNIX-1
-rwxr-xr-x 1 root root 114 Apr 21 06:38 UNIX-1
root@kali:~#
```

Changed Time (ctime) & Modified time (mtime)

```
Fragment: Address: 0 Number: 0 Size: 0
ctime: 0x5cbbb493:e2dcba54 -- Sun Apr 21 06:38:51 2019
atime: 0x5cbbb493:e2dcba54 -- Sun Apr 21 06:38:51 2019
mtime: 0x5cbbb493:e2dcba54 -- Sun Apr 21 06:38:51 2019
crtime: 0x5cbbb493:e2dcba54 -- Sun Apr 21 06:38:51 2019
Size of extra inode fields: 32
```

Create Time (Birth Time)

kali (vmware) က ကို စစ်ဆေးထားတဲ့ result ကိုပြသထားပါတယ်။

Videos (38)
Audio (70)
Archives (17294)
Databases (94)
Documents
HTML (4316)
Office (22)
PDF (119)
Plain Text (33602)
Rich Text (5)
Executable
By MIME Type
Deleted Files
File Size

Hex	Strings	Application	Indexed Text	Message	File Metadata	Results	Annotations	Other
File Name Allocation		Allocated						
Metadata Allocation		Allocated						
Modified		2019-04-20 22:58:13 MMT						
Accessed		2019-04-20 22:58:13 MMT						
Created		2019-04-20 22:58:13 MMT						
Changed		2019-04-20 22:58:13 MMT						

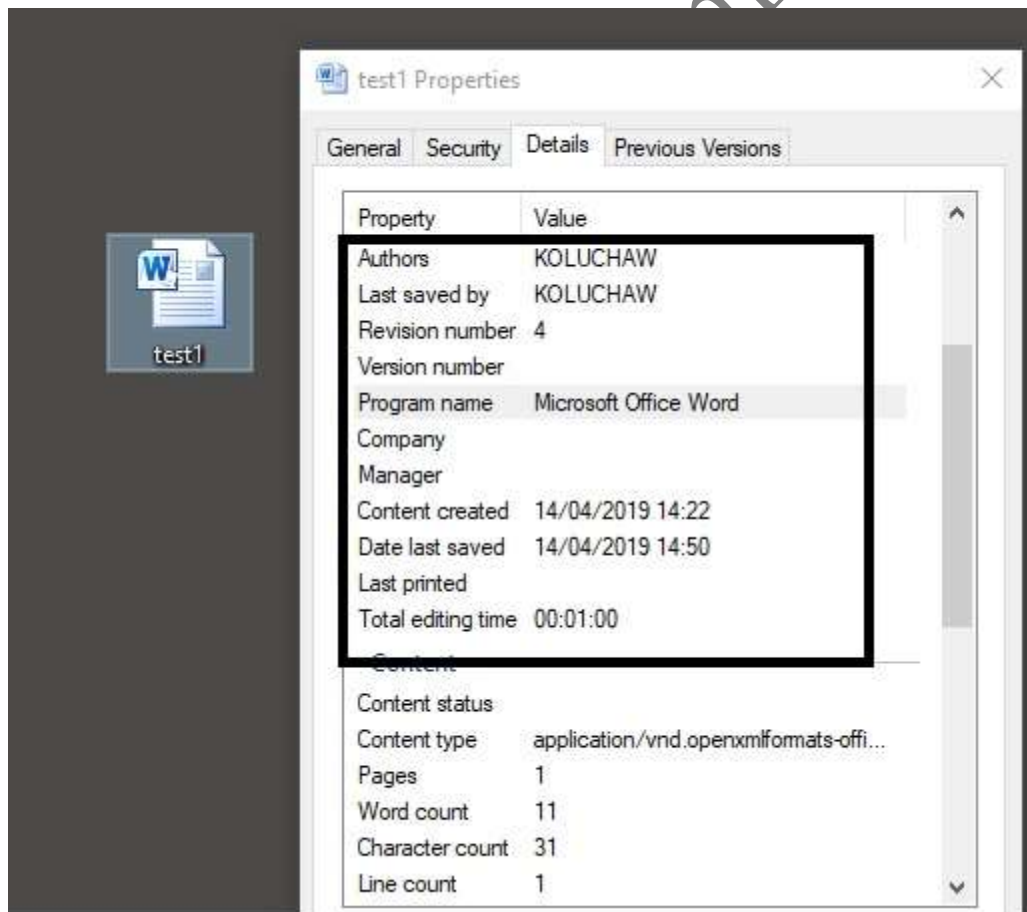
Metadata Forensics

Metadata ဆိုတာကတော့ data တွေနဲ့ပတ်သတ်ပြီးဖော်ပြတဲ့ အချက်အလက် (data) တစ်ခုပဲဖြစ်ပါတယ်။ Metadata က သက်ဆိုင်တဲ့ data တွေနဲ့တွဲပြီးရှိနေတတ်သလို အခြား file type အဖြစ်လဲရှိတတ်ပါတယ်။ တွေ့ရတာများတဲ့ metadata တွေကတော့ file extension, file size, file ကို create လုပ်တဲ့အချိန်, ဘယ်သူက Create လုပ်တယ်, ဘယ်စက်မှာ create လုပ်တယ်, ဘယ်အချိန်မှာ ဖွင့်တယ် ပြင်ဆင်တယ် စသည်ဖြင့်ရှိပါတယ်။ Metadata ကိုစစ်ဆေးဖို့အတွက် toolsတွေမလိုအပ်ပါဘူး

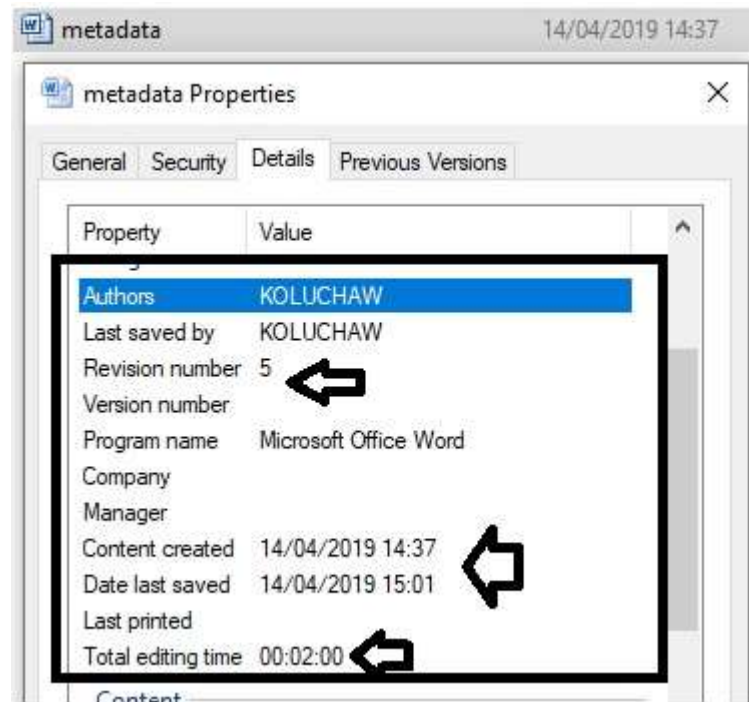
အချို့သော အနေအထားအတွက်လဲ သီးခြား tools တွေရှိပါတယ်။ Metadata ပြင်ဆင်ဖို့အတွက် သီးခြား Tools တွေလိုအပ်တဲ့အခါရှိသလို မလိုအပ်တာလဲရှိပါတယ်။ Anti Forensics tools တွေလဲရှိပါတယ်။

ဥပမာ အနေနဲ့ word file တစ်ခုကိုကြည့်ရအောင် word file ခေါ် Right Click ခေါ် Properties ခေါ် Detail မှာ test1 ရဲ့ Metadata ကိုတွေ့ရမှာဖြစ်ပါတယ်။ Author name မှာတော့ PC name ပေါ်မှာပါ။

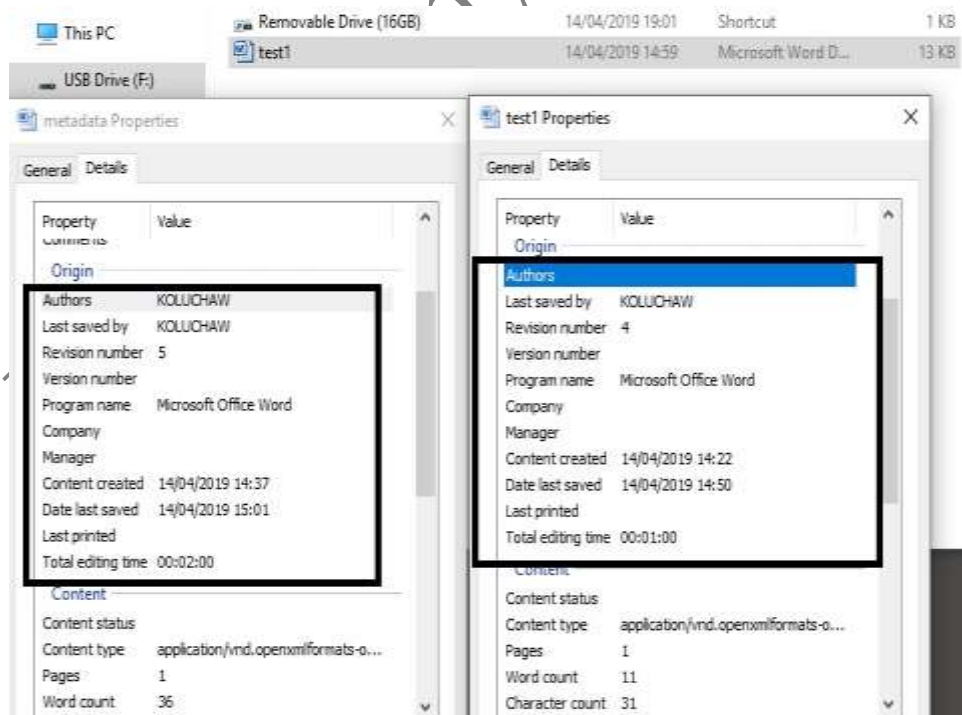
File ကို ဘယ်အချိန်မှာ နောက်ဆုံး save တယ်။ ဘယ်အချိန်မှာ Create လုပ်တယ် ဘယ်အချိန်မှာနောက်ဆုံး အသုံးပြုပြီး save တယ်။ edit လုပ်တာကြာချိန် နဲ့ ဘယ်နှစ်ကြိမ် ဖွင့်တယ် ပြင်တယ် ဆိုတာက အစမြင်ရမှာဖြစ်ပါတယ်



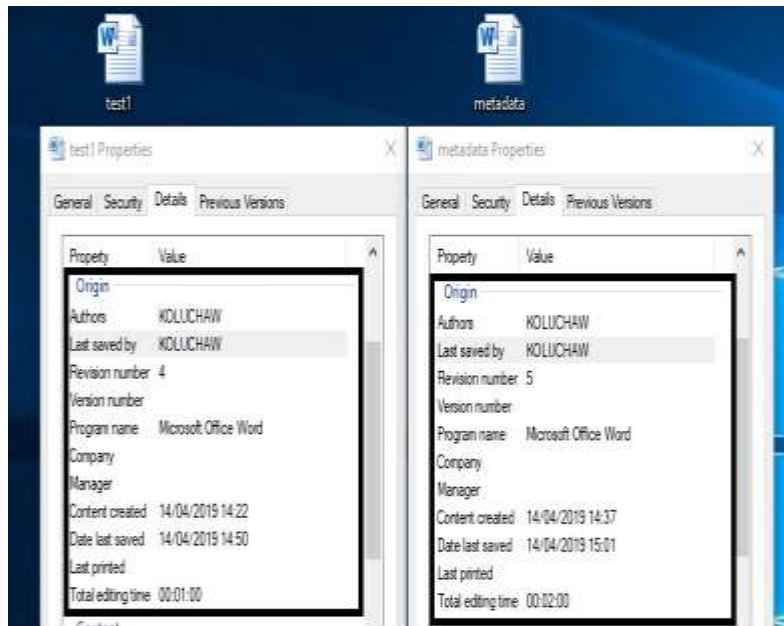
test1 ဆိုတဲ့ file ကို ကွန်ပျူတာထဲက Documents နေရာကို ပြောင်းပါတယ်။ metadata ဆိုပြီး file name ချိန်းလိုက်ပါတယ်။ ပြီးရင် Edit နည်းနည်းလုပ်ပြီး save လိုက်ပြီး metadata ကိုပြန်ကြည့်လိုက်ရင်ကွဲပြားခြားနားတာ တွေကိုတွေ့ရမှာပါ။



Test1 ကိုရော metadata ကိုရော stick ထဲပြောင်းထည့်လိုက်တဲ့အခါ မြင်ရတဲ့ metadata ဖြစ်ပါတယ်။



Test1 ကိုရော metadata ကိုရော ပြောင်းလိုက်တဲ့ ကွန်ပျူတာမှာ Edit လုပ်ပြီး ပြန်ကြည့်တဲ့ အခါမြင်ရတဲ့ Metadata အနေအထားပါ။



Test1file ကို googleDrive ပေါ်တင်ပြီး ပြန် Download ယူပါတယ်။ download လုပ်ထားတဲ့ Test1 ကိုဖွင့်ကြည့်တဲ့အခါမြင်ရတဲ့ metadata ဖြစ်ပါတယ်။ ThirdEyes ဆိုတဲ့ကွန်ပျူတာမှာနောက်ဆုံး save လာတယ် Author က KOLUCHAW စသည်ဖြင့်တွေ့ရမှာပါ။ pdf-metadata ကလဲအလားတူပါပဲ Microsoft word လို တော့ ပြည့်စုံခြင်းမရှိပါဘူး။

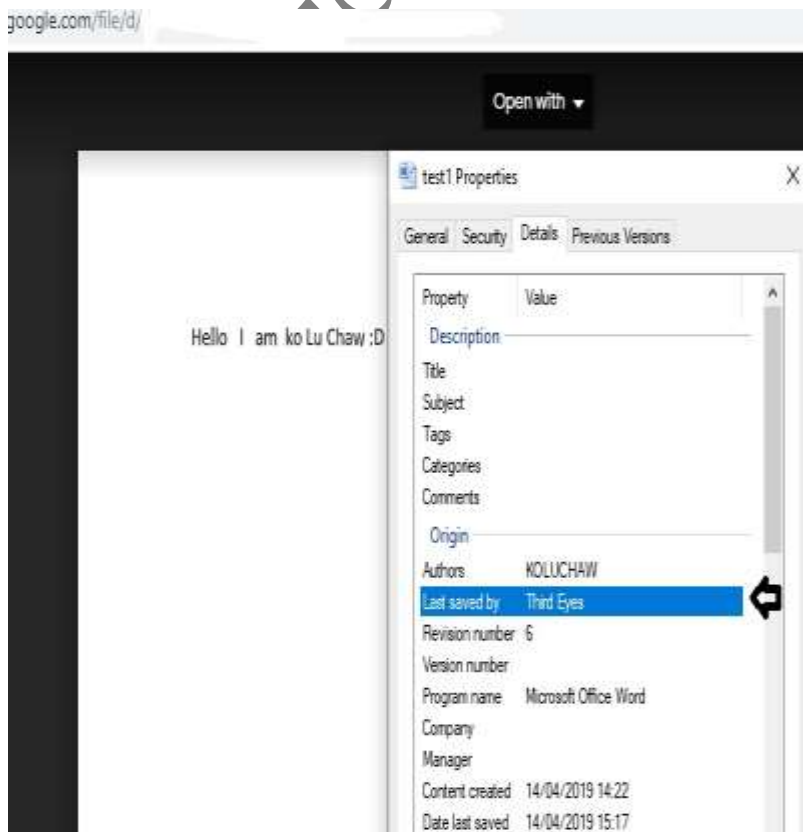


Image ,video,mp3 စတဲ့ metadata တွေကတော့ သူတို့က တင်ထားတဲ့ site ပေါ်မှာမူ တည်ပါတယ်။နောက်ပိုင်းကင်မရာတွေမှာ locationတွေဘာmodeကိုသုံးပြီးဘယ်လိုရိုက်တာလဲဆိုတဲ့အချက် အလက်တွေပါဝင်လာပါတယ်။Exif data တွေဖြစ်ပါတယ်။ ဒါကြောင့် image တွေရဲ့ အချက်အလက်ကို စစ်ဆေးနိုင်ပါတယ်။ဒါပေမဲ့ အချို့ image တွေကို တင်ထားတဲ့ site ကနေ image နဲ့ဆိုင်တဲ့ အချက်အလက်တွေကို user privacy အရသော်လည်းကောင်း ဖယ်ရှားထားပါတယ်။ example facebook site တွေမှာရှာဖွေမယ်ဆိုရင် resolution များတဲ့ပုံတွေမှာသာ တွေ့ရနိုင်ပါတယ်။

Image metadata စစ်ဆေးရန် Link များ

<http://exif.regex.info/exif.cgi>

<http://metapicz.com/#landing>

pdf word file metadata စစ်ဆေးရန်

<https://www.get-metadata.com/>

What Where Who When How

အခြား ဘာသာရပ်တွေမှာလဲ ဒီအမေး ဟာရှိပါတယ် Digital Forensics မှာဆိုရင် စစ်ဆေးသူရော .. တရားသူကြီးရောစစ်ဆေးရမဲ့ စဉ်းစားဆုံးဖြတ်ရမဲ့မေးခွန်းတွေဖြစ်ပါတယ်

What ဘယ်လိုအမှုမျိုးလဲ

Where ဘယ်နေရာမှာ ကျူးလွန်တာလဲ

Who ဘယ်သူက ကျူးလွန်တာလဲ

When ဘယ်အချိန်မှာ ကျူးလွန်တာလဲ

How ဘယ်လိုပုံစံနဲ့ကျူးလွန်တာလဲ

What

Cyber Crime Case ထဲက ဘယ်လိုအမှုမျိုးလဲ

အမှုအနေအထားနဲ့ ဖြစ်ရပ်ကိုကြည့်ခြင်းဖြစ်ပါတယ်

Where

မူခင်းဖြစ်တဲ့နေရာမှာ or အနီးတဝိုက်မှာ

ကျူးလွန်တာလား or

အဝေးကနေ ထိန်းချုပ်ပြီး ကျူးလွန်တာလား

Who

ဘယ်သူက ကျူးလွန်တာလဲ တစ်ယောက်ထဲဖြစ်နိုင်လား

ပူးပေါင်းမှုပါသလား (အမှုအနေအထားအရ)

When

ဘယ်အချိန်မှာကျူးလွန်တာလဲ

How

ဘယ်လိုပုံစံမျိုးနဲ့ ကျူးလွန်တာလဲ

(အမှုအနေအထားအရ ကျူးလွန်သော ပုံစံကွဲပြားခြားနားနိုင်ပါသည်)

ကျူးလွန်တဲ့အခါ Case ပုံစံအရ တစ်ယောက်ထဲက ကျူးလွန်နိုင်တာလား
ပူးပေါင်းသူပါဝင်ပါက ဘယ်လိုကျူးလွန်နိုင်မလဲ

Cyber Crime ကျူးလွန်နိုင်တဲ့ အခြေအနေတွေကတော့ Law မှာပါမှာပေါ့ ... Case ပေါ်မူတည်ပြီး Cyber Law အရ ပတ်သတ်နေလား တစ်ခြား ပြစ်မှုတွေနဲ့ရော ပတ်သတ်နေလားဆိုတာကတော့ Law Enforcement ကနေ စဉ်းစား ဆုံးဖြတ်ရမဲ့ အပိုင်းတွေဖြစ်ပါတယ် ဥပမာ အနေနဲ့ Case တွေကို အလျှင်းသင့်ရင် ဖော်ပြပေးပါမယ်။

Volume Shadow Copy (VSS) Forensics

Volume Shadow Copy (VSS) နှင့် System Restore Points Volume ခြားနားချက်ကတော့ system restore point မှာ OS ရဲ့ Good Condition အနေအထားကိုပဲရောက်ရှိစေမှာ ဖြစ်ပါတယ်။ သူနဲ့ တွဲလျက်ရှိတဲ့ Volume Shadow Copy မှာတော့ User ရဲ့ အရင်တစ်ချိန်ကရှိခဲ့တဲ့ File folder Web History , Registry , etc စတာတွေကိုရရှိနိုင်ပါတယ်။ Volume Shadow Copy (VSS) ကတော့ NTFS file System ကိုပဲ Support လုပ်ပါတယ်။ VSS ကို ရှာဖွေနိုင်တဲ့ Tools တွေ Free ရရှိနိုင်ပါတယ်။ vssadmin နဲ့လဲ cmd(admin) ဖြင့်ရှာဖွေနိုင်ပါတယ်။ လက်ရှိခေတ်စားနေတဲ့ Forensics Tools တွေမှာ Volume Shadow Copy (VSS) အတွက် သီးသန့် ရှာဖွေစစ်ဆေးလို့ရတာတွေရှိပါတယ်။ Example Encase

Encase မှာဆိုရင် အရင် ရေးထားတဲ့အတိုင်းပဲ forensics image ကို Write Protect device နဲ့တွဲဖက်ပြီးရယူ ပြီးရင် Image file ကို MD5 SHA တစ်ခုခုသုံးပြီး Hash value (True Copy) ဖြစ်အောင်လုပ်ပါမယ်။ ပြီးရင် Forensics WorkStation မှာ ခုနက ယူထားတဲ့ forensics image file ကို Mount လုပ်ပြီး Volume Shadow Copy (VSS) ကိုရှာဖွေရမှာဖြစ်ပါတယ်။ ရှာဖွေတဲ့အခါ VSS ရှိရင် VSS ဘယ်နှစ်ခုရှိလဲဆိုတာပြသပါမယ်။ Case အနေအထားအရ ကိုယ်လိုအပ်တဲ့ အချိန်ကာလ ကိုရှာဖွေ စစ်ဆေး ရမှာဖြစ်ပါတယ်

```
C:\Windows>cd ..
C:\>vssadmin list shadows /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.
```

Exchange PCB Board

Computer Forensics မှာ အဓိက ပါဝင်နေတဲ့ အလုပ်ဟာ Recovery ပြုလုပ်ခြင်းအပိုင်းလဲပါ ဝင်သလိုရောက်လာတဲ့ Computer တွေက အခြေအနေအမျိုးမျိုးကြောင့် ပျက်စီးနေတာလဲရှိပါတယ် HD Power On ကတည်းက Spindel Motor ကလည်ပတ်ခြင်းမရှိပါဘူး ကနဦးဆုံး စတင်စစ်ဆေးလိုက်တဲ့အချိန်မှာ HD PCB Fill ဖြစ်နေတာကိုတွေ့ရပါတယ် ... အခုအနေအထားအထိအတွင်းပိုင်းကိုဖြုတ်စရာမလိုသေးပါဘူးဒါကြောင့်

အသင့်ရှိပြီးသား Model တူ Firmware တူ RPM တူ တဲ့ အခြား HD က PCB ကို ဖြုတ်လဲပါ တယ်လဲပြီးတဲ့နောက်မှာ HD ကို Sata ကြိုးမတပ်သေးပဲ Power ပေးပါတယ် Spindel Motor လည်ပတ်ခြင်း ရှိမရှိနဲ့ အခြား False ရှိမရှိစစ်ဆေးရပါတယ်အဆင်မပြေရင် Bit by Bit Copy ကူးတဲ့အခါမှာ တစ်ဝက်တစ်ပျက်နဲ့ Fill ဖြစ်နိုင်ပါတယ်

First Responder Team Tasks in Cyber Crime

သက်သေခံပစ္စည်းများတစ်နေရာတည်းရှိနေချိန်..အခုအခြေအနေကတော့ First Responder Team က သက်သေခံအချက် အလက် တွေနဲ့ Device တွေက နေရာတစ်ခုထဲမှာရှိနေတဲ့ အနေအထားမှာ လုပ်ဆောင် ရမည့်အခြေခံအချက်အလက်များဖြစ်ပါတယ်။တည်နေရာတစ်ခုထဲဆိုတာ သက်သေခံအချက်အလက်တွေထဲက တစ်ချို့ဟာ Cloud အပိုင်း Data Center အပိုင်းမှာ ရှိမနေတဲ့ အချိန်ဖြစ်ပါတယ်။

ဖမ်းဆီးသိမ်းဆည်းရမည့် Case သဘာသဘာဝကိုနားလည်ခြင်း ဆိုတာကတော့ မိမိတို့သွားရောက် သိမ်းဆည်းရမဲ့ အမှုက ဘယ်လိုမူခင်းမျိုးလဲ ဒါဆိုရင် ဘယ်လိုသက်သေခံအချက်အလက်တွေက အရေးကြီးတယ် ဘယ်လို Device တွေရှိတတ်တယ်ဆိုတာကို First Responder Team ကနေကြိုတင်သိရှိပြီး First Responder Kits ကိုကြိုတင်ပြင်ဆင်ဖြည့်စွက်လို့ရပါမယ်။ (First Responder Kits မှာ Digital Crime အတွက် accessories မျိုးစုံပါဝင်ပါတယ်)

အခုအခြေအနေကတော့ သက်သေခံ အချက်အလက်တွေက နေရာတစ်ခုထဲမှာရှိနေတဲ့ အနေအထားပါ။

သက်သေခံ Device တွေက Desktop laptop လား သူနဲ့ ဆက်စပ်သုံးစွဲတဲ့ ဆက်စပ်ပစ္စည်းတွေရှိလား (eg. Printer) Printer သုံးစွဲပါက ထုတ်ထားတဲ့ စာရွက် ဓာတ်ပုံ အပိုင်းအစတွေရှိလား။ Lan ဒါမှမဟုတ် Internet နဲ့ချိတ်ဆက်ထားခြင်းရှိလားဆက်စပ်သုံးစွဲသော ပစ္စည်းများ

External Hard Drives, Removable Media, Thumb Drives, and Memory Cards,
Peripheral Devices,
Mobile Phone, tablet,
Potential Sources of Digital Evidence

သက်သေခံ Device တွေကို မပျက်စီးအောင်ကာကွယ်ခြင်းအပိုင်းမှာတော့ မူခင်းဖြစ်တဲ့နေရာမှာရှိနေတဲ့ လူတွေကို သက်သေခံပစ္စည်းတွေနဲ့ ဝေးကွာသောနေရာမှာနေခိုင်းရပါမယ်။ device တွေရဲ့အနေအထား ချိတ် ဆက်ထားမှုမှန်သမျှကို ဓာတ်ပုံမှတ်တမ်းယူရပါမယ်။

ဖမ်းဆီးတဲ့အချိန်မှာ Power on နေတဲ့ Device တွေကို Power on အနေအထားအတိုင်းထားရှိရမှာဖြစ်ပါတယ် Power Off အနေအထားနဲ့ရှိနေတဲ့ Device တွေကိုတော့ Power Off အနေအထားအတိုင်းပဲထားရှိရမှာဖြစ်ပါတယ်။ First Responder Team အဓိကလုပ်ဆောင်ရမည့်အချက်ကတော့ သက်သေခံပစ္စည်းမှ အချက်အလက်များ မပျောက်ပျက်အောင်ထိမ်းသိမ်းခြင်းနဲ့ ဆက်စပ်ပစ္စည်းများကို စုံလင်စွာ ရယူခြင်းတို့ပါဖြစ်ပါတယ်။ သိမ်း ဆည်းတဲ့နေရာမှာ ဓာတ်ပုံမှတ်တမ်းကလဲအရေးကြီးတဲ့နေရာမှာပါဝင်ပါတယ်။ ဥပမာ Network ချိတ်ဆက်ထား မယ်ဆိုရင် ဘယ် Device နဲ့ ချိတ်ဆက်ထားတယ် Switch Or router ရဲ့ ဘယ်အပေါက်မှာ ထိုးထားတယ်က အစမှတ်တမ်းတင်ရမှာဖြစ်ပါတယ်။ RAM ပါတဲ့ Device တွေဆိုရင် Power On အနေအထားနဲ့သိမ်းဆည်းနိုင် တာ အကောင်းဆုံးဖြစ်ပါတယ်။ Power ကို Forensics Lab ရောက်တဲ့အထိဆက်ပြီးပေးထားနိုင်ရင်အ ကောင်းဆုံးပါ။

Power On အနေအထားအတိုင်း ထားရှိရင် Live ဖြစ်နေတဲ့ System ကနေ အချက်အလက်တွေ ရယူနိုင်ဖို့ဖြစ်ပါတယ်။ အရင် Post တွေမှာ Live system ကနေ data collect လုပ်တာရေးထားပါတယ်။ သက်သေခံ Device များအား အချက်အလက်ထပ်မံမဖြည့်စွက်နိုင်အောင် Write Protect ပြုလုပ်ခြင်း

အပိုင်းကတော့ (First Responder Kits မှာပါဝင်တဲ့ Write Blocker Device တွေနဲ့ သက်သေခံ Device ကို အခြားသော အချက်အလက်များကို ထပ်မံဖြည့်လို့ မရအောင်ပြုလုပ်ခြင်းဖြစ်ပါတယ်။

သက်သေခံ Device များအား စနစ်တကျမှတ်တမ်းသွင်း ထုတ်ပိုး ပို့ဆောင်ခြင်းအပိုင်းကတော့ သိမ်းဆည်းတဲ့ Device တွေကိုမှတ်တမ်းသွင်းခြင်းနဲ့ Electronic ပစ္စည်းတွေဖြစ်တာကြောင့် Electronic Wave တွေနှောက်ယှက်မှုမဖြစ်အောင် ထုတ်ပိုးခြင်းအပိုင်းဖြစ်ပါတယ်။

First Responder Teamမေးမြန်းရမည့်မေးခွန်းများ (Example)

Crime တွင် Electronic Device ကိုအသုံးပြုသော လူများနှင့် Login and Password အင်တာနက်အသုံးပြုသော Email, Social Network Account နှင့် အလားတူအသုံးပြုသော Account များ၏ Password

Electronic Device ကိုအသုံးပြုခြင်းအကြောင်းနှင့်
အင်တာနက်အသုံးပြုပါက ISP နှင့် Service အမည်
Publi, Private Cloud အသုံးပြုမှု

သက်သေခံပစ္စည်းများတစ်နေရာတည်းတွင်မရှိတဲ့အခါလုပ်ရမည့်လုပ်ငန်းစဉ်ကို ပုံမှာပြသထားပါတယ်။

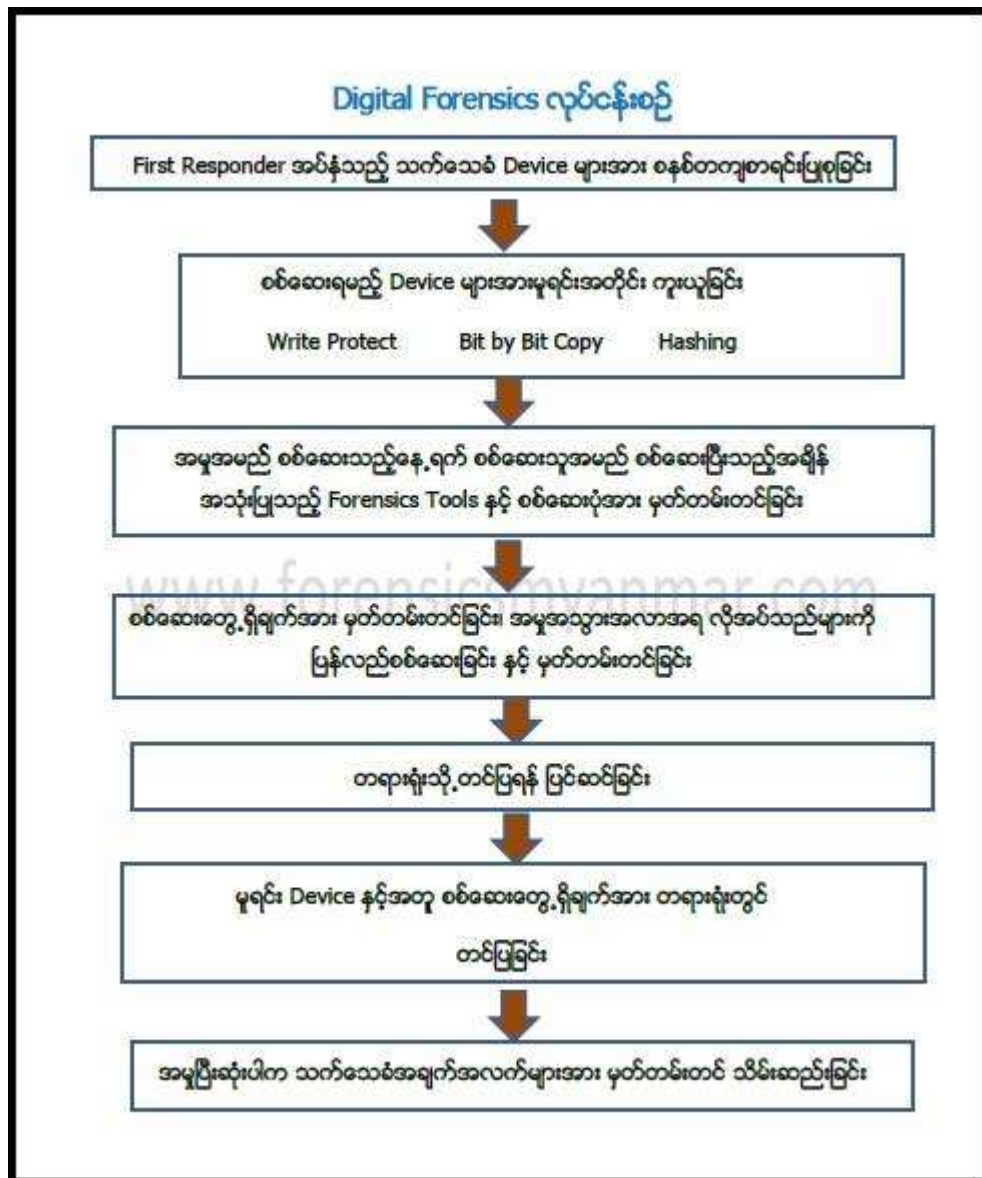
TRAIGE METHOD

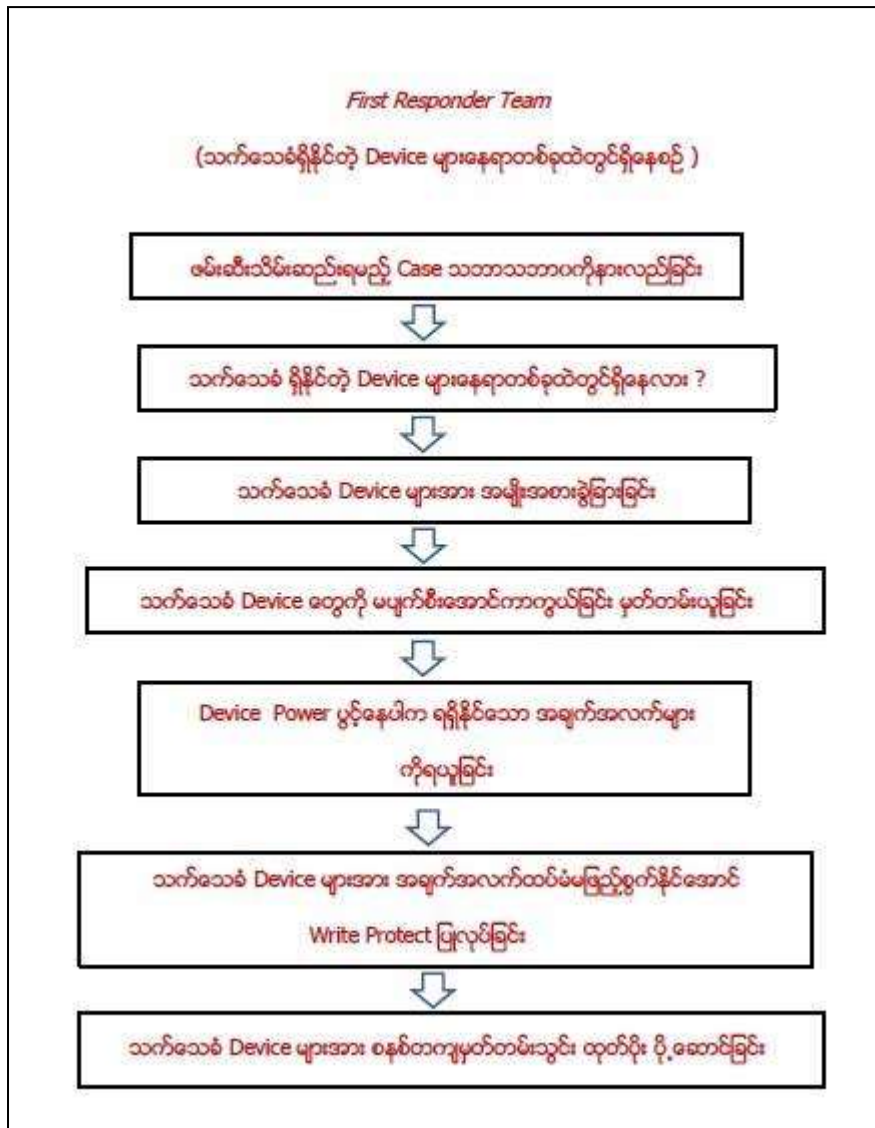
ဒီစကားလုံးက ဆေးပညာဝေါဟာရ ကနေလာတာပါအရေးကြီးတဲ့လူနာတွေ ဆေးရုံ Emergency အခန်းကို ရောက်လာတဲ့အခါ လူနာရဲ့ အခြေအနေပေါ်မူတည်ပြီးပြုစုကုသမှုပေးခြင်းဖြစ်ပါတယ်။

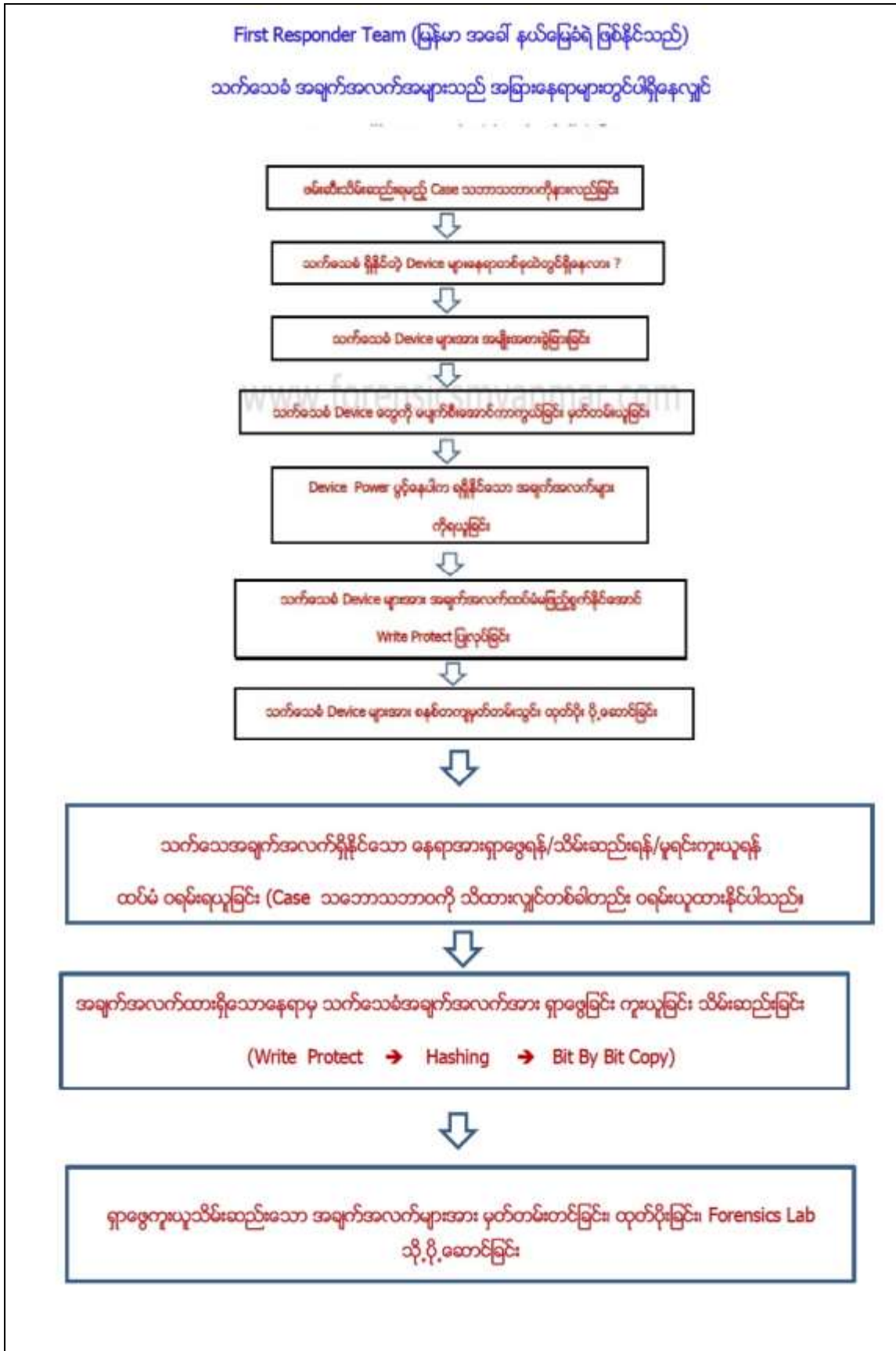
Digital Forensics မှာတော့တစ်မျိုးပါ First Responder Flow မှာက သက်သေခံအချက်အလက်က တစ်နေရာတည်း မှာရှိနေတာက တစ်နည်းWarrant ထုတ်ပြီးရှာဖွေယူနိုင်မဲ့နေရာဆို တစ်နည်း ဥပမာ Data Center တို့ Cloud တို့လိုနေရာတွေကိုရီးယားကားထဲကလို စာရွက်ထောင်ပြ ကဒ်ပြပြီး Warrant အရ ရှာဖွေပါတယ် ပြောသမျှကို တရားရုံးတွင်သက်သေခံတင်သွင်းမယ် ရှေ့နေငါးပိုင်ခွင့်ရှိပါတယ် ဆိုပြီးပြောမရ ... © Warrant ရဖို့တောင် အနိုင်နိုင် `ရလဲ Data Center က Server ကြီးကို မလာလို့မရ `

ပိုင်ရှင်နဲ့ မတွေ့ခင် CISSP လိုမျိုး ဥပဒေရော နည်းပညာပါ နားလည်တဲ့သူ နဲ့တင်တွေ့ပြီး ကိုယ့်ပါ အမှုပြန်ပတ်လာနိုင်တယ် ©

နောက်အခြေအနေတစ်မျိုးဖြစ်တဲ့Warrant မရနိုင်တဲ့အခြေအနေဖြစ်ပါတယ်။ ဥပမာ google facebook .. Mail ပို့ပြီး တောင်းရင် SPAM MAIL ဖုန်းဆက်ရင် Block List ထဲပါ ထည့်လိမ့်မယ် အရေးတယူလုပ်မှာမဟုတ်ပါဘူး ။ Power + Money ကလဲ Digital Forensics Investigation မှာ လူအရင်းအမြစ်လိုပဲ အရေးပါပါတယ်။အဲချိန်မှာ သုံးရမဲ့ Method က Triage Method ဖြစ်ပါတယ်ရရှိလာတဲ့ Information Source အနည်းငယ်နဲ့ပဲ လူသက်သေခံများနဲ့ စစ်ဆေးခြင်း အခြားသက်သေခံချက်များရယူခြင်း Special Forensics Tools များအသုံးပြုခြင်းတို့ဖြစ်ပါတယ်







Cyber Enable Crime and Cyber Dependent Crime

Electronic Crime, E-Crime, Technology Enable Crime, Hi-Tech Crime, Computer Crime, Computer Related Crime, Cyber Space Crime ဘယ်လိုပဲခေါင်းစဉ်သည်ဆိုပါစေ .. ဒါတွေနဲ့ ပတ်သက်ဆက်နွယ်နေတာတွေက မူခင်းအမြင်တစ်ခုနဲ့ တင်ကြည့်ရှုလို့မရနိုင်ပါဘူး ဥပဒေရေးရာ လူတွေရဲ့ စိတ်နေသဘောထားနဲ့ပတ်သတ်တာတွေ စီးပွားရေးနိုင်ငံရေးနဲ့ပတ်သတ်တာတွေကိုပါ ကြည့်ရှုရမှာဖြစ်ပါတယ်။ Non Border ဖြစ်နေတဲ့အတွက်ကြောင့်ဖြစ်ပါတယ်။

အရင်တုန်းက ဥပဒေအရ ယေဘုယျ ၃ မျိုးခွဲခြားထားပါတယ်
(နိုင်ငံအရ မတူနိုင်ပါ)

Computer ကို တစ်စိတ်တစ်ဒေသအသုံးပြုပြီး
ပြစ်မှုကျူးလွန်ခြင်း

Computer ကိုကြားခံ အသုံးပြုပြီး ပြစ်မှုကျူးလွန်ခြင်း
(ကြားခံ Computer မသိနိုင်တာလည်းရှိနိုင်ပါတယ်)

Computer ကို အသုံးပြုပြီး ပြစ်မှုကျူးလွန်ခြင်း

နောက်ထပ် ၂၀၀၆ ခုနှစ်မှာ Gordon နဲ့ Ford ခွဲခြားထားတာကတော့

Type 1

နည်းပညာကို ပုံမှန် သုံးစွဲနေကြအတိုင်းမဟုတ်ပဲ
ပုံမှန်ထက်ပိုအသုံးပြုကာ ပြစ်မှုကျူးလွန်ခြင်း
Eg. Hacking Methods

Type 2

နည်းပညာကို သုံးစွဲနေကြ ပုံမှန်အတိုင်း သုံးစွဲပြီး လူရဲ့
လုပ်ဆောင်မှုပါဝင်နေခြင်း
Eg. Online Gambling

Type 1 Type 2 နောက်မှာ AI နည်းပညာ Robotic နည်းပညာတွေတိုးတက်လာတာကြောင့် Type 3 ကိုထပ်မံ
ခွဲခြားပါတယ်

ကိုယ်တိုင်ခွဲခြမ်းစိတ်ဖြာတဲ့နည်းပညာကို အသုံးပြုပြီး
ပြစ်မှုကျူးလွန်ခြင်း

အခုနောက်ပိုင်းမှာတော့

Cyber Enable Crime, Cyber Dependent Crime
ဆိုပြီး ၂ မျိုးခွဲခြားလာပါတယ်

Cyber Enable Crime

Computer နဲ့ Data Store ဒါမှမဟုတ် Data ကို ပို့ဆောင်လက်ခံနိုင်တဲ့ Electronic Device တွေအသုံးပြုပြီး ကျူးလွန်ခြင်းဖြစ်ပါတယ်။ Internet အသုံးပြုသည်ဖြစ်စေ မပြုသည်ဖြစ်စေ အထက်ပါ Device တွေကိုအသုံးပြုပြီး ကျူးလွန်တာကိုသတ်မှတ်ပါတယ်။ ယခင်ကာလ ယခုကာလ မှာကျူးလွန်နေကျ ပြစ်မှုတွေဖြစ်ပါတယ်။ ဥပမာ အမုန်းစကားပြောတာ၊ ဘဏ် + photo video တွေဖြန့်ဝေတာ၊ Payment card တွေ ID တွေ ခိုးယူတာ၊ email အတုအယောင်နဲ့ လိမ်လည်တာ၊ သိက္ခာကျအောင်ပြောဆိုတာ (ယခင်ကျူးလွန်နေတဲ့မူရင်းတွေမှာ နည်းပညာ ပေါင်းစပ်ပြီး ကျူးလွန်တဲ့မူရင်းမျိုး ဖြစ်ပါသည်။)

Cyber Dependent Crime

Computer နဲ့ Data Store ဒါမှမဟုတ် Data ကို ပို့ဆောင်လက်ခံနိုင်တဲ့ Electronic Device တွေကိုအသုံးပြုပြီး Online ဒါမှမဟုတ် offline ကနေ လူမှုရေး နိုင်ငံရေးအကျိုးစီးပွားကိုများစွာပျက်စီးစေခြင်း၊ Computer နဲ့ Network System တွေရဲ့ data ဆက်သွယ်နေမှုတွေ Data သိုလှောင်ထားမှုတွေကို ထိခိုက်အောင်နှောင့်နှေးကြန့်ကြာအောင်ပြုလုပ်ခြင်း အဓိက CIA ကိုချိုးဖောက်ခြင်း

ဥပမာ DDoS DRDoS Phishing Virus and Malwares Hacktivist

First Responder Guide Android Device များကို သိမ်းဆည်းခြင်း

အရေးကြီးသည့် အချက်များကိုသာဖော်ပြထားပါသည်။

ရှာဖွေသိမ်းဆည်းရမဲ့ Mobile Device ဟာ Power ဖွင့်လျက်အနေအထားရှိနေပါက Power ကိုပိတ်ခြင်းမပြုပဲ Power Bank ဖြင့်ဆက်လက် Power ပေးထားရမည်ဖြစ်ပါသည်။ Volatile Information များအားရယူလိုသောကြောင့်ဖြစ်ပါသည်။ Encryption Keys သည် Volatile Data အတွင်းတွင်ရှိနေသောကြောင့်ဖြစ်ပါသည်။ Encryption Keys ရရှိလျှင် Physical Extraction Methods နှင့် Chip Off အတွက်အသုံးဝင်ပါသည်။

သံသယရှိသည်ထံမှ Mobile Device အား သိမ်းဆည်းပြီးနောက် Pin Code Password Pattern biometric အချက်အလက်များကို မေးမြန်းမှတ်သားခြင်း၊ Screen time out / Lock Timer များကို Never ပြုလုပ်ခြင်း၊ USB Debugging Mode အား တစ်ခါတည်း ဖွင့်ခြင်းများကို ပြုလုပ်ရမည်ဖြစ်ပါသည်။

Airplane mode ပြုလုပ်ရခြင်း ကတော့ အခင်းဖြစ်ရပ်သို့ သွားရောက်သိမ်းဆည်းရာတွင် Farady Case နှင့် Stronghold Bag များမပါရှိပါက kill Switch Feature နှင့် (Remote Wipe) မလုပ်နိုင်စေရန်ဖြစ်ပါသည်။

ဖုန်းအမျိုးအစားပေါ်မူတည်ပြီး Airplane mode တွင်ပြုလုပ်ထားသော်လည်း Wireless / Bluetooth များ On နေတတ်ပါသည်။ ထို့ကြောင့် သိမ်းဆည်းပြီးနောက် Airplane mode ကို On ထားရုံတင်မကပဲ Wireless / Bluetooth များကိုပါ ပိတ်ထားရမည်ဖြစ်ပါသည်။

kill Switch Feature နှင့် Remote Wipe Application များသည် Airplane mode ပေးထားသော်လည်း Battery လျော့နည်းလာခြင်း၊ Pin Password Pattern များကို သတ်မှတ်အကြိမ်ရေထက် ပိုဖွင့်မိပါက Mobile Phone အား Auto Wipe ဖြစ်စေပါသည်။ Farady Case နှင့် Stronghold Bag များထဲသို့ Mobile Device ထည့်သွင်းရသည့် နောက်ထပ်အကြောင်းအရာမှာ

မိုဘိုင်းဖုန်းအား Airplane mode ပေးထားသော်လည်း kill Switch Feature နှင့် Remote Wipe Application များသည် သတ်မှတ်ထားသည့် အခြေအနေကိုရောက်လျှင် Airplane mode ပေးထားသော်လည်း Wireless / Bluetooth များ Auto On ပါသည် .. ထို မိုဘိုင်းဖုန်းသို့ ချိတ်ဆက်ပြီး ဖျက်ဆီးနိုင်ပါသည်။ ထို့ကြောင့် Farady Case နှင့် Stronghold Bag များအသုံးပြုခြင်းဖြစ်ပါသည်။

Damage Mobile Device များ

ဓရ Chemical ထဲတွင် နစ်မြုပ် ပျက်စီးခြင်း၊

အစိတ်အပိုင်းများကွဲနေခြင်း၊

အပူကြောင့် မီးကြောင့်ပျက်စီးခြင်း

- ပျက်စီးရသည့်အကြောင်းအရာ အားမှတ်တမ်းတင်ခြင်း
- ကွဲကြွေနေသည့် အစိတ်အပိုင်းများကို စုစည်းခြင်း
- DNA/ လက်ဓမ္မရယူခြင်း
- Mobile Device အချက်အလက်များရယူနိုင်ပါက ရယူခြင်း
- Lab သို့ ပို့ဆောင်ရာတွင် စိုစွက်သည့်အကြောင်းအရာ (Eg. ဓရ၊ အက်ဆစ်) ကြောင့်ဖြစ်သည်ကို Label တပ်ခြင်း
- Lab သို့ ဆောလျင်စွာ ပို့ဆောင်ခြင်း

ဆက်စပ်သည့် အချက်အလက်များ ပစ္စည်းများရှာဖွေခြင်း

OTG Stick/ Laptop/Desktop/ Paper pieces/USB Stick /External; Hard Disk / Sim Card / Etc

Device Information ရယူခြင်း နှင့် document ပြုလုပ်ခြင်း

International Mobile Equipment Identity (IMEI),

Mobile Equipment Identifier (MEID),

Mobile Carrier

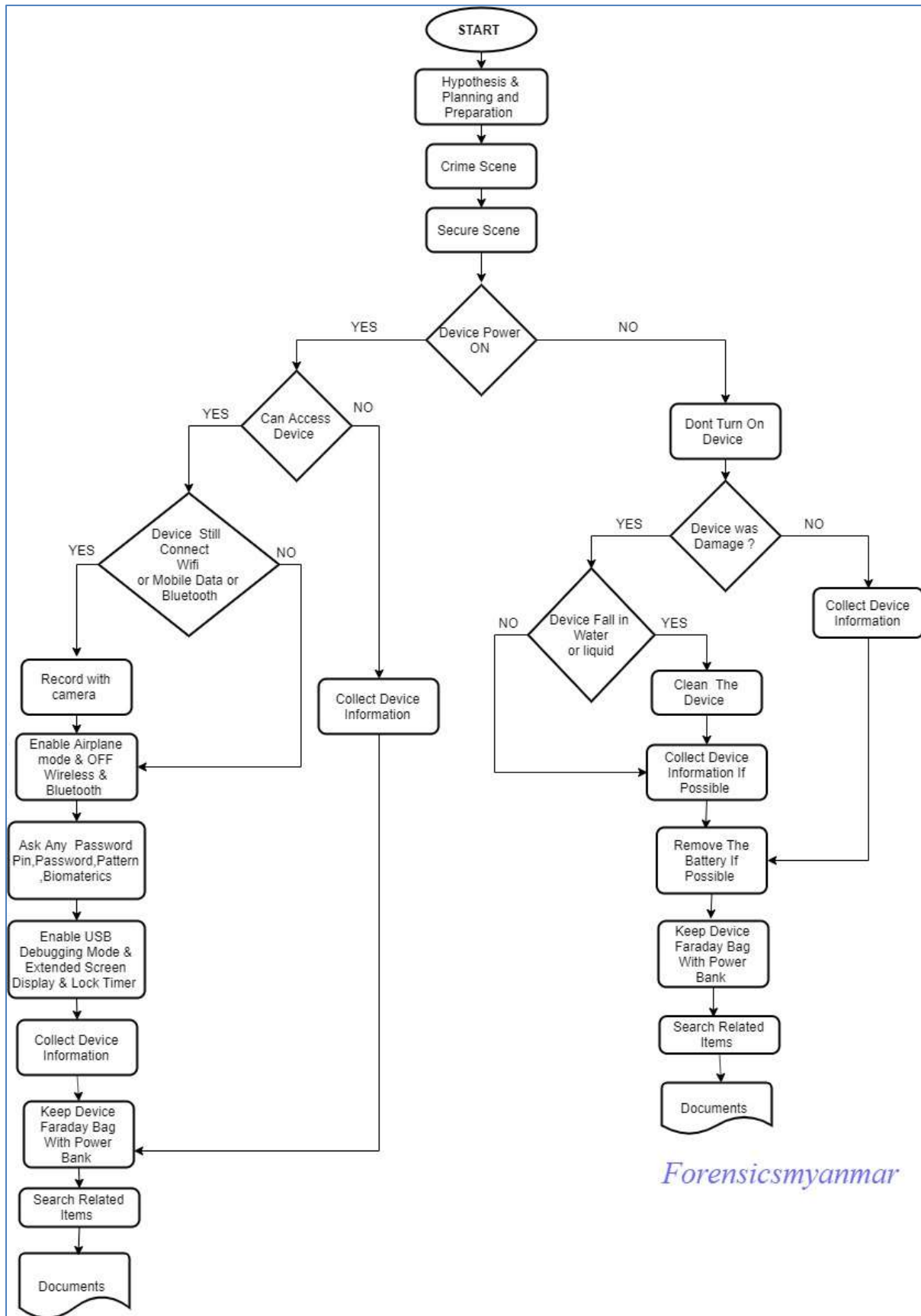
Mobile Phone Serial

Mobile Phone Condition (Good or Damage)

Pin Password Pattern

Etc

Forel



First Responder Guide
Android Device များကို သိမ်းဆည်းခြင်းပုံစံ

Embedded Universal Integrated Circuit Card “eUICC or (Embedded Sim (E SIM)

Mobile Phone Circuit board ထဲမှာ တစ်ခါတည်း ထည့်ထားသော Chip Set ဖြစ်ပါသည်။ Chip Set memory ပေါ်မူတည်ပြီး ကိုယ်သုံးချင်တဲ့ Network Operator တွေရဲ့ Profile ၁ ခု သို့မဟုတ် ၂ ခု တစ်ပြိုင်တည်းထည့်ထားနိုင်ပါသည်။ အရင် Sim Card မှာလိုပဲ သက်ဆိုင်ရာ Operator ကို ချိတ်ဆက်ရန် roaming ပြုလုပ်ရန် E-SIM Profile တွင် IMSI , ICCID MSISDN စသည့်အချက်အလက်တွေပါရှိမည်ဖြစ်ပါသည်။ E-Sim ထဲကို Profile အချက်အလက်ထည့်ပြီး ချိတ်ဆက်ရန် အတွက် သက်ဆိုင်တဲ့ Mobile Operator ကနေ ရောင်းချပေးတဲ့ Bar Code (သို့) QR Code(သို့) Application(သို့) Manual ရိုက်ထည့်နိုင်ပါသည်။

Telecom Profile တစ်ခုသာထည့်သွင်းနိုင်သော E-SiM အတွက်ဆိုရင် အခြား Operator ကိုပြောင်းသုံးချင် အရင်သုံးထားသော Profile ကိုဖျက်ပြီး ထည့်သွင်းရမည်ဖြစ်ပြီး Profile ၂ ခုအသုံးပြုနိုင်သော E-Sim ဆိုလျှင် မိမိ Profile တစ်ခုကို Disable /Enable ပြုလုပ်နိုင်မည်ဖြစ်ပါသည်။

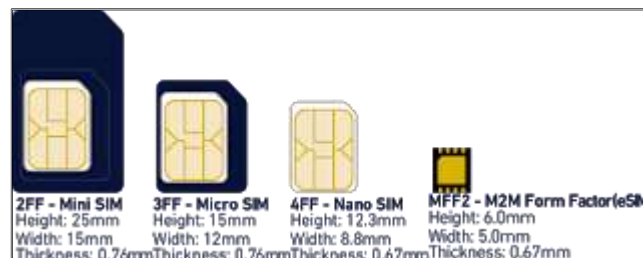
အခုလောလောဆယ်မှာ E -SIM အတွက် Forensics ပြုလုပ်ရန်နည်းလမ်းများစွာမရှိသေးသော်လည်း ဝယ်ယူသုံးစွဲသူ Information / Call Detail Record / IPDR / Location အချက်အလက်များကို Operator ထံမှ ရရှိနိုင်မည်ဖြစ်ပါသည်။

Mobile Forensics အတွက်ကတော့ E-SIM ထဲကနေ ဖျက်လိုက်တဲ့ Operator Profile အချက်အလက်တွေကို

E-Sim ထဲမှာ ပါဝင်သော Operation System (သို့) E-Sim Memory

Mobile Operation System (သို့) Mobile Phone ရဲ့ Memory (Power မပိတ်သောအခါ) (သို့) Backup (သို့) Cloud ထဲကနေ ရရှိနိုင်မည်ဖြစ်ပါသည် ။

(E-Sim အတွက် အကြမ်းမျှသာဖြစ်ပါသည်။)



Mobile Forensic Data Acquisition

Manual Extraction

သံသယရှိသူထံကနေ Mobile Device ကို စတင်သိမ်းဆည်းတဲ့အခါမှာ Mobile Device ကိုကြည့်ပြီး အသုံးပြုနေတဲ့ App / သိမ်းဆည်းနေတုန်းမှာ အချက်အလက်တွေကို ဖျက်နေတာတွေရှိနိုင်လား အသုံးပြုနေတဲ့ Telecom / Wireless AP စတာတွေကို ဓာတ်ပုံ ဗီဒီယို မှတ်တမ်းတင်ခြင်း၊ document ရေးသွင်းခြင်းတို့ဖြစ်ပါတယ်။

Logical Extraction

Mobile Device ထဲမှာ လက်တလောရှိနေတဲ့ Memory Storage ထဲကနေ System data / user data စတဲ့အချက်အလက်တွေကို ကူးယူခြင်းဖြစ်ပါတယ်။ ဖုန်းကို Back Up ယူတာနဲ့ဆင်တူပါတယ်။ အချို့သော ဖုန်း OS အမျိုးအစား Model အလိုက် Logical Extraction ကနေ Recovery ပြန်ရနိုင်ပါတယ်။

Physical Extraction

Mobile Device ထဲကနေ လက်တလော ရှိနေတဲ့ Memory Storage အပြင် ဖုန်းထဲမှာရှိနေတဲ့ Internal Memory / External Memory တွေထဲကနေ အချက်အလက်အားလုံးကို Bit by Bit Copy ကူးယူတာဖြစ်ပါတယ်။ (Recovery ပြန်လုပ်လိုတဲ့အတွက်ဖြစ်ပါတယ်)

Mobile phone အမျိုးအစား အလိုက် Physical Extraction ရနိုင်မရနိုင်တာတွေရှိပါသည်။

JTAG (Joint Test Action Group)

Mobile ph ထုတ်လုပ်သူများက Mobile Ph အမျိုးအစားတစ်ခုကို တပ်ဆင်ဆင်မထုတ်လုပ်ခင် တပ်ဆင်ထားတဲ့ Chip Set တွေ အမှားအယွင်းရှိ/မရှိစစ်ဆေးပါတယ်။ အဲလိုစမ်းသပ်စစ်ဆေးဖို့အတွက် အချို့သောဖုန်းများမှာ JTAG Connector က ဖုန်းရဲ့ Circuit Board မှာပါရှိပါတယ်။ မပါရှိရင်

Memory Chip ကို ရှာပြီး JTAG လုပ်ဖို့ အတွက် Wire ချိတ်ဆက်ဖို့ရှာပါမှာဖြစ်ပါတယ်။ TAP (Test Access Port) လုပ်တယ်လို့လဲခေါ်ပါတယ်။ချိတ်ဆက်လို့ရလျှင် Mobile Ph ရဲ့ Processor ကနေ Memory Chip ကို Command ပေးပြီး Full Memory Record ရအောင်ပြုလုပ်ပါတယ်။ Lock ဖြစ်နေတဲ့ ဖုန်းတွေတစ်စိတ်တစ်ပိုင်းပျက်စီးနေတဲ့ဖုန်းတွေကို စစ်ဆေးဖို့ပြုလုပ်ရခြင်းဖြစ်ပါသည်။ (JTAG ပြုလုပ်ဖို့အတွက် သီးသန့် adapter/ Reader/ software တွေလိုအပ်ပါတယ်။ JTAG ပြုလုပ်ဖို့ ဖုန်းအမျိုးအစားများရဲ့ cpu memory တွေအကြောင်းကို နားလည်တတ်ကျွမ်းသူလဲ လိုအပ်ပါတယ်။ ဈေးနှုန်းကလဲ တော်တော်များပါတယ်။

Chip OFF

JTAG အဆင့်နဲ့မရရင် ဖုန်းကနေ Memory Chip ကိုဖြုတ်ပြီး Chip Set Reader မှာတင်ပြီး Memory Chip ထဲက အချက်အလက်တွေကို ဖတ်တာဖြစ်ပါတယ်။ JATG လိုပဲ သီးသန့် ကျွမ်းကျင်သူတွေအပြင် အသုံးပြုရတဲ့ပစ္စည်းတွေလဲ လိုအပ်ပါတယ်။ ငွေကြေးကုန်ကျမှုပိုမိုများပြားပါတယ်။ Android 6.0 အထက်ဆိုရင် Encryption ကြောင့် အနည်းငယ် အခက်အခဲရှိပါတယ်။

Micro Read

နောက်ဆုံးနည်းလမ်းဖြစ်ပါတယ်။ ကျွမ်းကျင်တဲ့ ပညာရှင်များ လိုအပ်ပါတယ်။ Memory Chip အပေါ်လွှာကို ဖယ်ရှားပြီး Chip ထဲက Gate တွေကို Microscope နဲ့ဖတ်တာဖြစ်ပါတယ်။ Gate တွေရဲ့ အနေအထားကိုကြည့်ပြီး Binary ကနေ HEX , HEX ကနေ data သို့ ပြောင်းလဲခြင်းဖြစ်ပါသည်။

SIM CARD FORENSIC

SIM CARD FORENSIC

SIM (Subscriber Identity Module) တစ်ခုမှာ CPU၊ RAM၊ OS၊ EEPROM၊ ROM တို့ပါရှိပါတယ်။ SIM ရဲ့ File System ကတော့ Tree ပုံစံဖြစ်ပါတယ်။ ပါဝင်တဲ့ File System တွေကတော့ Master File (MF), Dedicated Files (DF) နှင့် Elementary Files (EF) တို့ဖြစ်ပါတယ်။ ပုံမှာပြထားတဲ့အတိုင်း Master File (MF) က ကျန်တဲ့ File 2 ခုရဲ့ Root ဖြစ်ပါတယ်။ Child directories တွေကတော့ Dedicated Files (DF) နှင့် Elementary Files (EF) တို့ဖြစ်ပါတယ်။ ပုံပါအတိုင်း Dedicated Files (DF) ရဲ့အောက်မှာ Elementary Files (EF) တွေအများကြီးရှိပါသည်။ Sim Card တစ်ခုပြုလုပ်တော့မယ်ဆိုရင် ISO/IEC 7816 အတိုင်းလိုက်နာရမှာဖြစ်ပါတယ်။ ISO/IEC 7816 မှာအပိုင်း ၁၅ ပိုင်းပါဝင်ပါတယ်။

UMTS 3G SIM Card ကနေစပြီး Video Call ပါဝင်လာ
ပါတယ်။ Data encryption Method နဲ့ Storage ပိုင်းမှာ
မြင့်မားလာပါတယ်။

SIM Card Forensics လုပ်ရာမှာသိရှိထားရမည့် အသုံးအနှုန်းတွေကတော့ အောက်မှာဖော်ပြထားပါတယ်။

Integrated Circuit Card Identifier uniquely identifies (ICCID) မှာ

Issuer Identification Number (IIN)

Account Identification Number (AIN) ဆိုပြီး ၂ မျိုးပါဝင်ပါတယ်။

(ICCID ကို Sim Card ဝယ်ယူတဲ့အခါ Sim Card အခွံပေါ်မှာ နံပါတ်နဲ့ရော Barcode နဲ့ပါဖော်ပြထားပါသည်။

MPT တွင် Sim Card ပေါ်တွင်ပါရှိပါသည်။

Issuer Identification Number (IIN) အများဆုံးဂဏန်း ၇ လုံးပါဝင်ပါတယ်။

ပထမဆုံး ဂဏန်း ၂ လုံးကတော့ Major Industry Identifier (MII) ဖြစ်ပါတယ်။ ဒုတိယ ဂဏန်း ၂ သို့မဟုတ် ၃

လုံးကတော့ Country Code (CC) ဖြစ်ပါတယ်။ တတိယ ဂဏန်း ၂ လုံး သို့မဟုတ် ၃ လုံး ကတော့ Mobile

Network Code (MNC) ဖြစ်ပါတယ်။ Issuer Identifier Number (IIN) လို့လဲခေါ်ပါတယ်။

Account Identification Number (AIN)

ကျန်တဲ့ ဂဏန်းတွေကတော့ Sim card ကိုင်ဆောင်သူနဲ့ပတ်သတ်တဲ့ အချက် အလက်တွေဖြစ်ပါတယ်။ Sim

card ကိုထုတ်လုပ်တဲ့ရက်စွဲ Home Location Register (HLR) နဲ့ Sim Card နံပါတ်တွေဖြစ်ပါတယ်။

ဥပမာ MPT Sim Card ရဲ့ ICCID ကို ကြည့်ကြည့်လျှင်

89 95 01 41 7315 0258567 4 ဆိုပြီး ဂဏန်း အလုံး ၂၀ ရှိတာတွေ့ရမှာဖြစ်ပါတယ်။

89 ကတော့ Major Industry Identifier (MII) ဖြစ်တဲ့ Telecommunication ကိုရည်ညွှန်းတာဖြစ်ပါတယ်။ 95

ကတော့ မြန်မာနိုင်ငံရဲ့ Country Code (CC) ဖြစ်ပါတယ်။ 01 ကတော့ MPT ရဲ့ Mobile Network Code

(MNC) ဖြစ်ပါတယ်။

ကျန်တဲ့ဂဏန်းတွေဖြစ်တဲ့ 41 7315 0258567 ကတော့ Account Identification Number (AIN) ဖြစ်ပါတယ်။

နောက်ဆုံးဂဏန်း 1 ကတော့ barcode ဖတ်ရင် Error မဖြစ်အောင်အတွက်ဖြစ်ပါတယ်။

နောက်ထပ်ဥပမာ MYTEL SIM Card ရဲ့ ICCID ကတော့

89 95 09 000600 8831487 1 ဆိုပြီး ဂဏန်းအလုံး ၂၀ တွေ့မြင်ရမှာဖြစ်ပါတယ်။ MYTEL ရဲ့ Mobile

Network Code (MNC) မှာ 09 ဖြစ်ပါတယ်။

မြန်မာနိုင်ငံမှာလက်ရှိအသုံးပြုနေတဲ့ GSM Sim Card တွေမှာ

899501..... = MPT , 899505 = Ooredoo, 899506.... Telenor , 89950... = Mytel ဖြစ်ပါတယ်။

International Mobile Subscriber Identifie (IMSI)

(IMSI) မှာတော့ ဂဏန်း 15 လုံးပါရှိပါသည်။ Mobile Phone နဲ့ Cell Tower ဆက်သွယ်မှုရရှိရန်အတွက်

အဓိကထားသုံးပါတယ်။ ရှေ့ဆုံးဂဏန်း ၃ လုံးကတော့ Mobile County Code (MCC) ဖြစ်ပြီး နောက် ၂ ဂဏန်း

၂ လုံးကတော့ Mobile Network Code (MNC) ဖြစ်ပါတယ်။ ကျန်တဲ့ ဂဏန်း ၁၀ လုံးကတော့ Mobile

Identification Number (MSIN) ဖြစ်ပါတယ်။ ဥပမာ

MPT (IMSI) = 414 01 0050258547

414 ကတော့ မြန်မာနိုင်ငံမှာရှိတဲ့ Telecom အားလုံးအတွက် နံပါတ်ဖြစ်ပါတယ်။

01 ကတော့ MPT ရဲ့ ကတော့ Mobile Network Code (MNC) ဖြစ်ပါတယ်။

Telenor (IMSI) = 414 06 0511957386

06 ကတော့ Telenor ရဲ့ Mobile Network Code (MNC) ဖြစ်ပါတယ်။

Mobile Station International Subscriber Directory Number (MSISDN)

(MSISDN) ကတော့ အရှင်းဆုံးနဲ့အလွယ်ဆုံးပြောရရင် မိမိလက်ရှိသုံးနေ တဲ့ဖုန်းနံပါတ်ဖြစ်ပါတယ်။ မိမိဖုန်းသို့

အဝင် Call အတွက်အသုံးပြုတာဖြစ်ပါတယ်။ ဂဏန်းအားဖြင့် 15 လုံးရှိပါသည်။ ဥပမာ ပြည်ပကနေ မြန်မာနိုင်ငံ

ရန်ကုန်က လိုင်းဖုန်းကို ခေါ်မယ်ဆိုရင် +95 1 444444 ဆိုပြီးခေါ်ဆိုရမှာဖြစ်ပါတယ်။ +95 ကတော့ Country Code ဖြစ်ပြီး +1 ကတော့ National Destination Code ဖြစ်ပါတယ်။ Mobile ph ကိုခေါ်ဆိုမယ်ဆိုရင်လဲဒီသဘောတရားပဲဖြစ်ပါတယ်။

SPN and SDN (Service Provider Name and Service Dialing Numbers) ကတော့ Telecom Operator အမည်နဲ့ Customer Care ph no တို့ဖြစ်ပါတယ်။

Temporary Mobile Subscriber Identity(TMSI)

(TMSI) ကတော့ အသုံးပြုသူက လက်ရှိအသုံးပြုချိတ်ဆက်နေတဲ့ Cell Tower ကနေ နေရာပြောင်းရွှေ့တဲ့အခါမျိုးမှာ ပြောင်းလဲတဲ့နေရာကနေ အနီးဆုံး ဒါမှမဟုတ် လိုင်းဆွဲအား အကောင်းဆုံး Cell Tower ကိုပြန်ပြီးချိတ်ဆက်တဲ့အခါမျိုးမှာ IMSI အစားအသုံးပြုတာဖြစ်ပါတယ်။

Phone Contact တွေကို Sim Card မှာ သိမ်းထားရင် Abbreviated Dialing Numbers (ADN) ၊ LND (Last Numbers Dialed) တွေဖြစ်တဲ့ အကြိမ်ရေအများဆုံးခေါ်ထားတဲ့ Call Log တွေ နောက်ဆုံးခေါ်ထားတဲ့ Call Log တွေကို ရရှိနိုင်မှာဖြစ်ပါတယ်။

Short Message Service (SMS)

(SMS) တွေကို Si Card ထဲမှာသိမ်းဆည်းထားခဲ့ရင် ပြန်လည်ရရှိနိုင်မှာဖြစ်ပါတယ်။ Sim Card ထဲမှာ သိမ်းဆည်းထားပြီးနောက် ဖျက်ထားခဲ့ရင်လည်ပြန်လည် ရယူနိုင်ပါသည်။

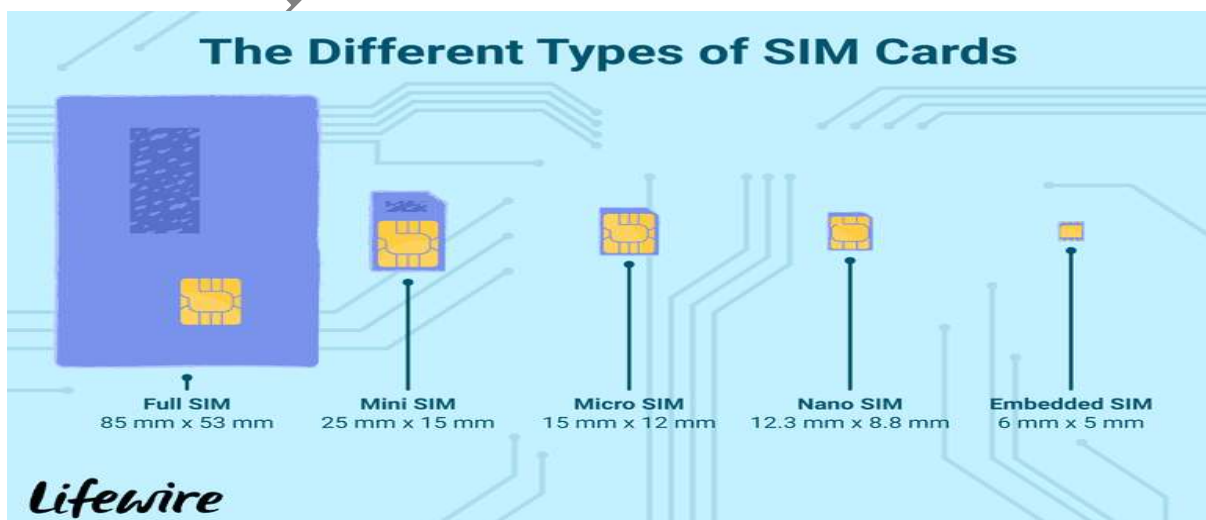
Sim Card ရဲ့ Dedicated Files (DF) ထဲမှာပါဝင်တဲ့ Location Information (LOCI) ကနေ the Location Area Identifier (LAI)၊ Mobile Country Code (MCC)၊ Mobile Network Code (MNC)၊ the Location Area Code (LAC)၊ Routing Area Code (RAC) ၊ the Routing Area Information (RAI)၊ Location Update Information တို့ကို ရရှိနိုင်ပါတယ်။ MCC,MNC, LAC RAC RAI တို့အား (Call Detail Record ရေးတဲ့အချိန်မှာ ထည့်သွင်းရေးသားသွားပါမည်)

Sim Card ကို စစ်ဆေးတဲ့အခါမှာတော့ Sim Card Adapter (R/W) ထဲကို Sim Card အသစ်တစ်ခုနဲ့ (Bit by Bit Copy) ကူးယူပြီး မူရင်းကိုမပျက်စီးစေပဲ ကူးယူထားတဲ့ Sim Card ထဲက အချက်အလက်တွေကို စစ်ဆေးတာဖြစ်ပါတယ်။ စစ်ဆေးမှုအခြေအနေအပေါ်မူတည်ပြီး Sim Card ထဲမှ အချက်အလက် ၄၀ ကနေ ၂၅ ချက်အထိ စစ်ဆေးနိုင်ပါသည်။စစ်ဆေးသူ၏ ကျွမ်းကျင်မှု အသုံးပြုသော ဆက်စပ်ပစ္စည်းများပေါ်တွင်လည်းမူတည်ပါသည်

သံသယရှိသူသည် မှုခင်းဖြစ်ချိန်မှာ နေရာတွင် ရှိ မရှိ

အလီဘိုင်လိမ်လည်ထွက်ဆိုမှု

အာမခံလိမ်လည်မှု အစရှိသည့် မှုခင်းများတွင် အသုံးပြုနိုင်ပါသည်



First Responder Guide

မူခင်းနှင့်ဆက်စပ်သည့် CCTV မှတ်တမ်းများကို သိမ်းဆည်းခြင်း

DVR အမျိုးအစားများ

Stand-Alone Embedded Digital Video Recorder (DVR)
 Network Video Recorder (NVR)
 Hybrid Digital Recorder
 PC Based DVR
 Personal Computer (By using Video Recording Software)
 Server Based (Eg- Network Attach Storage) (NAS)

ရုပ်ထွက်အကောင်းဆုံး Video ကိုရယူနိုင်မှသာ Forensics ပြုလုပ်ရာတွင် လွယ်ကူရှင်းလင်းပြတ်သားစွာ လုပ်နိုင်မည်ဖြစ်ပါသည်။ ကူးစရာမပါလို့ (Monitor ပေါ်က Video ကို ဖုန်းဖြင့်ရိုက်ယူခြင်း၊ ဓာတ်ပုံရိုက်ခြင်းများကို မပြုလုပ်ရပါ) (Resolution ကျဆင်းစေပါသည်)
 (မူခင်းနှင့် အခြေအနေပေါ်မူတည် ပြီး DVR တစ်ခုလုံးရယူနိုင်ရင်တော့ အကောင်းဆုံးဖြစ်ပါသည်)

Compression Methods

=====

CCTV မှရရှိတဲ့ Video နဲ့ Audio Record တွေကို သိမ်းဆည်းတဲ့ File Format ကတော့ သုံးထားတဲ့ DVR , NVR Type တွေအပေါ်မူတည်ပြီး type မျိုးစုံရှိပါတယ်။ ကွန်ပျူတာပေါ်မှာ တိုက်ရိုက် ဖွင့်လို့ရတဲ့ type တွေရှိသလို တိုက်ရိုက် ဖွင့်လို့မရတဲ့ type တွေလဲရှိပါတယ်။ CCTV Forensics လုပ်တဲ့နေရာမှာ compression Methods တွေသိထားရင် အထောက်အကူဖြစ်နိုင်ပါတယ်။ CCTV ကနေကနဦးမှတ်တမ်းတင်လိုက်တဲ့ Video Raw Data က File Size ကြီးပါတယ် ဒါ့ကြောင့် Cable/Wireless ပေါ်မှာ ပို့လွှတ်ဖို့ရော , Data သိမ်းထားဖို့အတွက်ရော အခက်အခဲရှိပါတယ်။ ဒီလိုအခက်အခဲမဖြစ်အောင် compression Methods တွေကို အသုံးပြုပါတယ်။ ယနေ့လက်ရှိအသုံးအများဆုံး Compression Methods ကတော့ H.264 ဖြစ်ပါတယ်။ ယခင်ကအသုံးပြုနေတဲ့ MPEG-4 , MJPEG တွေထက် Video Compression ပိုင်းမှာ ပိုကောင်းပါတယ်။ Storage ပမာဏ အနည်းဆုံးနဲ့ Video Quality အကောင်းဆုံးဖြစ်အောင် Compression လုပ်ပေးပါတယ်။ Transmit ပိုင်းမှာလဲ bandwidth (bit rate) အနည်းဆုံးနဲ့ transmit လုပ်ပေးပါတယ်။

CCTV Record ပြုလုပ်ရန် လိုအပ်သောပစ္စည်းများ

=====

Record ယူမည့်နေရာ၏ CCTV System တပ်ဆင်ထားပုံ Hard ware အပေါ်မူတည်ပြီး Record ယူရာတွင် လိုအပ်မည့်ဆက်စပ်ပစ္စည်းများမှာ

Laptop

Record ယူမည့်နေရာ၏ CCTV System တပ်ဆင်ထားပုံ Hard ware အပေါ်မူတည်ပြီး လို/ မလို) Eg .. Lan ပေါ်မှကူးယူမည်ဆိုလျှင်လိုအပ်မည်ဖြစ်ပါသည်။ ကွန်ပျူတာနှင့် ဆက်စပ်ပစ္စည်းများဖြင့်သည့် DVD USB Or Wireless Mouse / Keyboard , Lan Cable , Power Extension / Marker Pan များလိုအပ်ပါသည်။

USB Extension

အချို့ DVR များတွင် Mouse (or) Wireless Mouse တပ်ဆင်ရန် USB Port တစ်ခုသာပါဝင်ပါသည်။ DVR တွင် USB Port တစ်ခုသာပါရှိလျှင် Memory Stick ဖြင့်ကူးယူမည်ဆိုပါက USB Extension လိုအပ်ပါသည်။

External Hard Disk (or) USB Stick (Minimum 16 GB (ကူးယူမည့် အချိန်ပေါ်တွင်မူတည်ပါသည် (HD CCTV Record 1 နာရီစာသည် 1.5 GB မှ 2 GB ကြားတွင်ရှိပါသည်။)

လိုအပ်လျှင် DVR အမျိုးအစားကိုကြည့်ပြီး Mobile Data ဖွင့်ပြီး Google မှာ DVR Specification ကိုရှာပါ။

CCTV Record ရယူခြင်း

=====

မူရင်းဖြစ်ရပ်အားရှင်းလင်းစွာမြင်နိုင်သည့် Camera Channel အားရွေးချယ်ခြင်း၊ ဆက်စပ်နိုင်သည့် မြင်ကွင်း Channel များအားရွေးချယ်ခြင်း (Physical CCTV တပ်ဆင်ထားပုံအရ ကွဲပြားနိုင်ပါသည်) (တစ်နေရာတည်းမှ မဟုတ်ပဲ အခြားနေရာများမှ CCTV Record များပါလိုအပ်နိုင်ပါသည်)

DVR System Information

(Eg. DVR တွင်တပ်ဆင်နိုင်သော Channel ။ လက်ရှိတပ်ဆင်ထားသော Camera အရည်အတွက်။ DVR ထဲတွင်လက်ရှိ သိမ်းဆည်းထားသော Channel အရည်အတွက်။ System Login PassWord (admin/user)။

မိမိလိုအပ်သော Record သည် DVR Record ထဲတွက်ရှိမရှိ။ မူရင်းပေါ်မူတည်ပြီး ရယူရမည့် Record နေ့ရက် အချိန်အတိုင်းအတာ (မှ- ထိ)

Record ရယူမည့် Video အား USB/External Hard Disk/DVD or Laptop အတွင်းသို့ ကူးယူမည့်နည်းလမ်း / File Type

- ကူးယူရာတွင် DVR Setting မှ Compression Methods အားမပြောင်းလဲဘဲ လက်ရှိ Compression Methods ဖြင့်သာ ကူးယူရပါမည်။ Resolution ကောင်းစေရန်အတွက် Compression Methods မပြောင်းလဲရပါ။ (Save ထားသော Video ပေါ်တွင် သက်ရောက်မှုမရှိပါ Documented တွင်သာ မှတ်တမ်းထားရမည်ဖြစ်ပါသည်)

- USB Stick ဖြင့်ကူးယူမည်ဆိုပါက USB Stick အား Fomant ချပြီးမှ ကူးယူရပါမည်။ USB Stick မကောင်းလျှင် အချိန်ကြာပါသည်။

Documented ပြုလုပ်ရမည့်အချက်များ

=====

- DVR Location Address (ph No, Etc ...)
- DVR အမျိုးအစား
- DVR model, and serial number
- DVR password & username(s)

-ချိတ်ဆက်ထားသော Camera အရည်အတွက် ၊ တပ်ဆင်နိုင်သော Camera အရည်အတွက်

- DVR တွင်ပေါ်နေသော အချိန်နှင့် လက်ရှိ အချိန် ကွားခြားခြင်း ရှိမရှိ

(ကွာခြားပါက DVR မှ အချိန်အား မပြောင်းလဲဘဲ လက်ရှိအချိန်နှင့်ကွာခြားမှုအား မှတ်သားပါ)

- DVR တွင် အသံပါ သွင်းယူနိုင်ခြင်းရှိမရှိ လက်ရှိသွင်းယူထား၊ မထား

-DVR တွင်လက်ရှိ အနေအထားအရ ပထမဆုံး Video သိမ်းဆည်းထားသည့်အချိန်

- DVR အတွင်းရှိ Hard Disk Storage ပမာဏ

- Storage Over Write ပြုလုပ်ထားခြင်း ရှိမရှိ

(ပြုလုပ်ထားပါက Over Write ဖြစ်ရန် သတ်မှတ်ထားသည့် အချိန်ကာလ Eg- 7 day or 30 days)

- DVR System settings ဖြစ်သည့် -

Image Video quality (i.e. high, medium, low)

Frames per second

Recorded image/frame size (e.g. 320 x 240)

Alarm , motion trigger settings for cameras

DVR firmware version

- *System logs (Important)*

Camera ဖြင့်သော်လည်းကောင်း / DVR အမျိုးအစားအရ Log File Save ခြင်းဖြင့်သော်လည်းကောင်း ရယူနိုင်ပါသည်။

- DVR နှင့် CCTV Camera များတပ်ဆင်ထားပုံအား ပုံကြမ်း (သို့) Camera မှတ်တမ်းရယူရပါမည်။

(NVR မှ ရယူရာတွင်လည်း နည်းလမ်းသိပ်မကွဲပြားပါ) (LAN/Wireless/DHCP အခြေခံသာလိုအပ်ပါသည်)

DVR တစ်ခုလုံးအားသိမ်းဆည်းခြင်း

=====

DVR တစ်ခုလုံးအား သိမ်းဆည်းရန်လိုလောက်သည့် အခြေအနေများမှာ

- DVR အတွင်းမှ Video Record များဖျက်ထားသည်ဟု သံသယရှိလျှင်

- အခြားအခြေအနေများဖြင့်ဆက်စပ်ရယူရမည့် အနေအထားရှိလျှင်

- DVR တစ်ခုလုံး သိမ်းဆည်းရမည့် အနေအထားရှိလျှင်

- ကူးယူရမည့် Video Size ပမာဏ အရမ်းများနေလျှင်

- ကူးယူဖို့ပြင်ဆင်ရာတွင် (သို့) ကူးယူနေစဉ် နည်းပညာ အခက်အခဲရှိလာလျှင်

- DVR အား Recovery ပြုလုပ်ရန် လိုအပ်သည်ဟု ယူဆလျှင်

- အခြားသာ မသင်္ကာစရာ အချက်အလက်ရှိလာလျှင်

